

日本国特許庁
JAPAN PATENT OFFICE

#2

JC979 U.S. PTO
09/934764
08/23/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 8月25日

出願番号

Application Number:

特願2000-255840

出願人

Applicant(s):

株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月27日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特2001-30359

【書類名】 特許願

【整理番号】 A000004877

【提出日】 平成12年 8月25日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 電子機器及び接続制御方法

【請求項の数】 19

【発明者】

 【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

 【氏名】 伊藤 隆文

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

 【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子機器及び接続制御方法

【特許請求の範囲】

【請求項 1】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器であって、

第 1 の状態と第 2 の状態を切り換え可能なスイッチと、

このスイッチが第 1 の状態に設定されている場合には、上記特定の識別コードによる認証を禁止する認証禁止手段と、

上記スイッチが第 2 の状態に設定されている場合には、上記特定の識別コードによる認証を許可する認証許可手段と

を具備したことを特徴とする電子機器。

【請求項 2】 上記スイッチが第 2 の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第 2 の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証を禁止する制御手段と

を具備したことを特徴とする請求項 1 記載の電子機器。

【請求項 3】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段と、

第 1 の状態と第 2 の状態を切り換え可能なスイッチと、

このスイッチが第 1 の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する変更禁止手段と、

上記スイッチが第 2 の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を許可する変更許可手段と

を具備したことを特徴とする電子機器。

【請求項 4】 上記スイッチが第 2 の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第 2 の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する制御手段と、

を具備したことを特徴とする請求項 3 記載の電子機器。

【請求項 5】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段と、

他の機器から接続要求があったときに、当該機器の機器コードが上記機器コード記憶手段に記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて記憶する認証エラー記憶手段と、

この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否する制御手段と

を具備したことを特徴とする電子機器。

【請求項 6】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項 7】 上記リンク情報登録手段は、各機器それぞれのリンク情報に

対応付けて、各機器それぞれの最終接続時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その最終接続時刻の最も古い機器のリンク情報を削除することを特徴とする請求項 6 記載の電子機器。

【請求項 8】 上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、その登録時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その登録時刻の最も古い機器のリンク情報を削除することを特徴とする請求項 6 記載の電子機器。

【請求項 9】 上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、各機器それぞれの接続回数を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その接続回数の最も少ない機器のリンク情報を削除することを特徴とする請求項 6 記載の電子機器。

【請求項 10】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

上記特定の識別コードを記憶する識別コード記憶手段と、

他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項 11】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する電子機器であって、

上記他の機器と接続するための交換可能な無線通信ユニットと、

この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段と、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項 1 2】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器に用いられる接続制御方法であって、

上記電子機器の本体に第 1 の状態と第 2 の状態を切り換え可能なスイッチを設けておき、

このスイッチが第 1 の状態に設定されている場合には、上記特定の識別コードによる認証を禁止し、

上記スイッチが第 2 の状態に設定されている場合には、上記特定の識別コードによる認証を許可することを特徴とする接続制御方法。

【請求項 1 3】 上記スイッチが第 2 の状態に設定されてから所定時間経過したか否かを検知したか否かを判断し、

上記スイッチが第 2 の状態に設定されてから所定時間経過した場合には、上記特定の識別コードによる認証を禁止することを特徴とする請求項 1 2 記載の接続制御方法。

【請求項 1 4】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

他の機器との間で接続を行うための各種管理情報を記憶したメモリを備え、
上記電子機器の本体に第 1 の状態と第 2 の状態を切り換え可能なスイッチを設けておき、

第 1 の状態と第 2 の状態を切り換え可能なスイッチと、

このスイッチが第 1 の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を禁止し、

上記スイッチが第 2 の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を許可することを特徴とする接続制御方法。

【請求項 1 5】 上記スイッチが第 2 の状態に設定されてから所定時間経過したか否かを判断し、

上記スイッチが第 2 の状態に設定されてから所定時間経過した場合には、上記メモリに記憶されている各種管理情報の変更を禁止することを特徴とする請求項 1 4 記載の接続制御方法。

【請求項 1 6】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

リンクの張られた他の機器それぞれの機器コードを第 1 のメモリに記憶しておき、

他の機器から接続要求があったときに、当該機器の機器コードが上記第 1 のメモリに記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行い、

この認証により認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて第 2 のメモリに記憶し、

この第 2 のメモリに記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否することを特徴とする接続制御方法。

【請求項 1 7】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を作成し、

このリンク情報を該当機器と対応付けてメモリに登録し、

このメモリによるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除することを特徴とする接続制御方法。

【請求項 1 8】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

上記特定の識別コードを第 1 のメモリに記憶しておき、

他の機器から接続要求があったときに当該機器に対して上記第 1 のメモリに記憶された特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を作成し、

このリンク情報を該当機器と対応付けて第 2 のメモリに登録し、

上記第 1 のメモリに記憶された特定の識別コードが変更された場合には、上記第 2 のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。

【請求項 1 9】 他の機器との間でリンクを張る際に特定の識別コードによる認証を要し、上記他の機器と接続するための交換可能な無線通信ユニットを備えた電子機器の接続制御方法であって、

上記無線通信ユニットの固有の識別コードを第 1 のメモリに記憶しておき、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を上記メモリに記憶された無線通信ユニットの識別コードに基づき作成し、

このリンク情報を該当機器と対応付けて第 2 のメモリに登録し、

上記無線通信ユニットが交換された場合には、上記第 2 のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、他の機器との間でデータ通信を行う無線通信機能を備えた電子機器及び接続制御方法に関する。

【0002】

【従来の技術】

近年、I r D A、B l u e t o o t h、H o m e R F等のパーソナルエリアの無線通信システムが注目されている。特に、B l u e t o o t hやH o m e R Fは、I r D Aのような赤外線通信方式と比較して、指向性がない、透過性が高いなどの長所を有しており、今後の発展、普及が大いに期待されている。なお、B l u e t o o t hは、近距離の無線通信規格であり、2.4GHz帯のI S M (Industrial Science Medical) バンドを用いて10m以内あるいは100m以内の無線通信を実現するものである。

【0003】

B l u e t o o t h、H o m e R F等の無線通信システムは、同時に複数の機器との接続が可能である他に、I r D Aのような赤外線通信方式と比較して伝送距離が例えば10～100mと比較的長いということも大きな特徴の一つである。これは使い勝手の向上という利点もあるが、その反面、無線により外部から容易にアクセスできるため、無線通信システムのセキュリティ、秘話性の確保等に関しては十分に注意する必要がある。

【0004】

一般的な無線通信システムのセキュリティ方式としては、特許第2872996号の公報に記載されている方式が知られている。これは、電子鍵と無線端末装置からなるセキュリティシステムにおいて、セキュリティを強化するために、同一鍵の連続使用を禁止し、紛失や盗難に対しての安全性を高めたものである。

【0005】

また、B l u e t o o t hでは、以下のようなユーザ認証によるセキュリティ方式が採用されている。

【0006】

B l u e t o o t hにおけるユーザ認証は、機器に設定するユニークな認証パスワードと、この認証パスワード及び機器固有のID（IEEEが管理、発番する48ビットのアドレス）等により作成される暗号鍵との2つにより管理されている。上記認証パスワードはPIN（Personal Identification Number）コードと呼ばれ、任意の文字列で構成される。上記暗号鍵はリンクキーと呼ばれ、ユーザ認証の他にデータの暗号化などにも用いられる。

【0007】

今、機器Aが機器Bに対してアクセスする場合を考える。

【0008】

機器Aと機器Bが初めて接続される状況においては、機器Aは機器BのPINコードを入力する必要がある。機器Aから入力されたPINコードが正しいと判定された場合には、機器Bは認証可としてリンクを開設して接続を許可する。このとき、機器Bは自身のPINコード及び機器AのIDに乱数を掛け合わせるなどして機器Aのリンクキーを作成し、これを機器AのIDと共にリンクキーテーブルに保存しておく。なお、リンクキーを作成する場合に、各機器間で互いにリンクキーを交換する相手のPINコードや自身のIDも用いる。

【0009】

一方、機器Aが以前に機器Bに接続されたことがあれば、既に機器Aのリンクキーが上記リンクテーブルに登録されているので、PINコードの入力を省いて、上記リンクキーによる認証を行う。

【0010】

【発明が解決しようとする課題】

B l u e t o o t hを利用した機器として様々なものがあり、その1つとして、モデムアクセスポイントと呼ばれる回線接続機器がある。このモデムアクセスポイントは公衆回線への接続機能を備えたものであり、これにB l u e t o o t hの通信機能を付加すれば、他のB l u e t o o t h対応機器との間で無線による接続が可能となる。したがって、外部機器からモデムアクセスポイントに無線によりアクセスすれば、外部機器側ではモジュラーケーブルの接続を必要とせず

に、公衆回線に接続してインターネット等の利用を受けることができる。この場合、モデムアクセスポイントへのアクセスには、上述したPINコードまたはリンクキーによる認証が行われており、認証可と判定された外部機器のみがモデムアクセスポイントへの接続が許される。

【0011】

しかしながら、モデムアクセスポイントのPINコードが何らかの手段で本来の利用者以外の者に知られた場合、そのPINコードを使用してモデムアクセスポイントに不正アクセスする可能性がある。モデムアクセスポイントの場合には、公衆回線の接続によって回線使用料金が生じるため、不正アクセスは重大な問題となる。

【0012】

また、通常、モデムアクセスポイントは目立たない場所に設置され、かつ、電源が常時ONになっていることが多い。このため、管理者が知らないうちに、外部からモデムアクセスポイントに不正アクセスする可能性が高い。

【0013】

本発明は上記のような点を解決するためになされたもので、他の機器からの不正アクセスを防止してセキュリティを確保することのできる電子機器及び接続制御方法を提供することを目的とする。

【0014】

【課題を解決するための手段】

すなわち、本発明の請求項1に係る電子機器では、他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、第1の状態と第2の状態を切り換え可能なスイッチが第1の状態に設定されている場合には、上記特定の識別コードによる認証が禁止され、また、上記スイッチが第2の状態に設定されている場合には、上記特定の識別コードによる認証が許可されるので、他の機器のユーザは、上記特定の識別コードを知っていても、上記スイッチを第1の状態に設定操作しない限り、当該機器とのリンクを張ることができないことになる。

【0015】

また、本発明の請求項2に係る電子機器では、前記請求項1に係る電子機器に

あって、上記スイッチが第2の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証は禁止されるので、上記スイッチが第2の状態に設定されたままでも、所定時間経過の後には他の機器とのリンクを張ることができないようになる。

【0016】

また、本発明の請求項3に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段を有し、第1の状態と第2の状態を切り換え可能なスイッチが第1の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が禁止され、また、上記スイッチが第2の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が許可されるので、他の機器の不正ユーザがこの電子機器と接続できても、上記スイッチを第1の状態に設定操作しない限り、上記他の機器との接続のための各種管理情報の変更操作はできないことになる。

【0017】

また、本発明の請求項4に係る電子機器では、前記請求項3に係る電子機器にあって、上記スイッチが第2の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更は禁止されるので、上記スイッチが第2の状態に設定されたままでも、所定時間経過の後には上記他の機器との接続のための各種管理情報の変更操作はできないようになる。

【0018】

また、本発明の請求項5に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段を有し、他の機器から接続要求があったときに、当該機器の機器コードが前記機器コード記憶手段に記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証が行われ、認証エラーと判定された場合には、当該機器の機器コードとその

エラー回数とが対応付けられて認証エラー記憶手段に記憶される。そして、この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求が拒否されるので、同一機器からの不正な接続の試みはできないようになる。

【0019】

また、本発明の請求項6に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合には、その登録リンク情報のうち、例えば最終接続時刻の最も古い機器のリンク情報（請求項7）、又は登録時刻の最も古い機器のリンク情報（請求項8）、又は接続回数の最も少ない機器のリンク情報（請求項9）という不要なリンク情報が判定されて削除されるので、新たな接続機器とのリンク情報を接続可能性の低い機器のリンク情報と代えて登録できることになる。

【0020】

また、本発明の請求項10に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記特定の識別コードを記憶する識別コード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記特定の識別コードの書き換え後は当該新たな識別コードを知らないユーザによって他の機器との間でリンクが張られるのを防止できることになる。

【0021】

また、本発明の請求項 1 1 に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記他の機器と接続するための交換可能な無線通信ユニットと、この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記無線通信ユニットの交換後はそのユニット固有の識別コードに基づくリンク情報を作成し登録し直さないと、他の機器とのリンクが張れないことになる。

【 0 0 2 2 】

【発明の実施の形態】

以下、図面を参照して本発明の一実施形態を説明する。

【 0 0 2 3 】

図 1 は本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図である。図 1 では、公衆回線の接続機能を備えた回線接続機器（以下、アクセスポイントと称す）1 0 と、このアクセスポイント 1 0 との間で無線通信を行うパーソナルコンピュータ（以下、パソコンと称す）1 0 0 が示されている。

【 0 0 2 4 】

アクセスポイント 1 0 およびパソコン 1 0 0 には、無線通信カードとして、Bluetooth の無線通信規格に従った PC カード（以下、BT-PC カードと称す）2 0 が脱着自在に装着されている。アクセスポイント 1 0 およびパソコン 1 0 0 は、この BT-PC カード 2 0 を装着することで、互いに無線によるデータ通信が可能となる。

【 0 0 2 5 】

パソコン 1 0 0 は、ここではアクセスポイント 1 0 にアクセスする外部機器として用いられる。このパソコン 1 0 0 の本体 1 1 4 には、キーボード 1 1 2 や液

晶表示パネル 116、カードスロット 118 が設けられている。

【0026】

アクセスポイント 10 は、モジュラケーブル 12 を介して公衆回線 11 に接続され、パソコン 100 から無線送信されたデータを公衆回線 11 に転送すると共に公衆回線 11 から入力されたデータをパソコン 100 に無線送信する。

【0027】

図 2 乃至図 6 にアクセスポイント 10 の構成を示す。

【0028】

図 2 はアクセスポイント 10 の分解斜視図、図 3 はアクセスポイント 10 を縦置きで使用した状態を示す斜視図、図 4 はアクセスポイント 10 の背面側を示す斜視図、図 5 はアクセスポイント 10 を横置きで使用した状態を示す斜視図、アクセスポイント 10 の底面側を示す斜視図である。

【0029】

図 2 乃至図 6 に示すように、アクセスポイント 10 は、例えば合成樹脂等によって形成されたほぼ矩形状の機器本体 14 を備えている。この機器本体 14 は、僅かに湾曲した前面 14a、この前面と対向したほぼ平坦な背面 14b、対向する一対の側面 14c、上面 14d、および底面 14e を有している。そして、機器本体 14 の底面 14e および背面 14b はそれぞれ第 1 および第 2 設置面を構成している。

【0030】

アクセスポイント 10 は、図 3 および図 4 に示すように、底面 14e を机面上等に載置することにより機器本体 14 を縦置きとして使用し、あるいは、図 5 に示すように、背面 14b を机面上等に載置することにより機器本体 14 を横置きとして使用することができる。また、背面 14b には、ピンやフック等を掛けるための 2 つの係合凹所 16 が形成され、これらの係合凹所 16 を利用することにより、機器本体 14 をその背面が壁と対向した状態で壁掛け式としても使用することができる。

【0031】

機器本体 14 の一方の側面 14c には、押しボタン式の電源スイッチ 18 が設

けられている。他方の側面 1 4 c には、R S 2 3 2 C コネクタ 2 2 および電源接続用の A C アダプタ端子 2 3 が設けられている。また、機器本体 1 4 の前面 1 4 a には、アクセスポイント 1 0 の動作状態を示す表示部として、複数の L E D 2 4 が並んで設けられている。動作状態としては、例えば、電源オン（POWER）、送信（SD）、受信（RD）、オフフック（OH）、後述する B T - P C カード 2 0 のスタンバイ／アクティブ（STB/ACT）状態等を表示する。

【 0 0 3 2 】

機器本体 1 4 の上面 1 4 d には、着脱自在な透明カバー 1 5 と、後述するカードスロット 2 6 のカード挿入口 2 8 およびイジェクトボタン 3 0 が設けられている。また、図 6 から分かるように、底面 1 4 e には、アクセスポイント 1 0 を公衆回線 1 1 に接続するためのモジュラケーブル 1 2 を接続可能な 2 つのモジュラジャック 3 2、左右一対のスライドスイッチ 3 4 a、3 4 b、1 つのロータリスイッチ 3 5 が設けられている。

【 0 0 3 3 】

底面 1 4 e には、その周縁部に沿ってスカート部 3 6 が立設され、その一部には切欠 3 7 が形成されている。このスカート部 3 6 は、機器本体 1 4 を縦置きとして使用する際に脚部として機能する。上記モジュラジャック 3 2 に接続されたモジュラケーブル 1 2 は、切欠 3 7 を通して外部に引き出される。従って、モジュラジャック 3 2 にモジュラケーブル 1 2 を接続した状態で機器本体 1 4 を縦置きとして使用する場合でも、モジュラケーブル 1 2 が邪魔になることなく、スカート部 3 6 により機器本体 1 4 を安定して支持することができる。

【 0 0 3 4 】

機器本体 1 4 内には、保持部として機能するカードスロット 2 6 が設けられ、このカードスロットのカード挿入口 2 8 は機器本体の上面 1 4 d に開口している。そして、このカードスロット 2 6 には、カード挿入口 2 8 を通して、B T - A C カード 2 0 を脱着自在に装着可能となっている。

【 0 0 3 5 】

次に、B T - P C カード 2 0 の構成について説明する。

【 0 0 3 6 】

図7はBT-PCカード20の斜視図、図8はBT-PCカード20の分解斜視図である。

【0037】

図7および図8に示すように、BT-PCカード20は、PCMCIAの規格に準拠したカード本体40と、カード本体の一端側から突出している共にBT規格に準拠した送受信部42とを備えている。カード本体40は、合成樹脂からなるほぼ矩形状の枠体43を有する。この枠体43は、カード本体40内のカード基板44の周縁部を支持している。カード基板44の一端にはコネクタ45が取り付けられ、また、カード基板の他端部はカード本体40から突出している。

【0038】

カード基板44の一方の表面、ここでは上面44a上には、複数の電子部品46が実装されている。また、カード基板44の他端部上面には、送受信部42を構成するアンテナ部46、送受信時に点灯するLED47およびヘッドフォン、マイクロフォン等を接続するためのヘッドセット部48が設けられている。

【0039】

そして、カード基板44の上面および下面は、枠体43に嵌合された一对の金属カバー50a、50bにより、他端部を除いて覆われている。

【0040】

また、送受信部42は合成樹脂からなるキャップ51を有し、このキャップ51はカード本体40の他端に嵌合され、カード基板44の他端部、およびこの他端部上面に実装されたアンテナ部46、LED47、ヘッドセット部48を覆っている。

【0041】

上記BT-PCカード20において、コネクタ45が設けられている前端はカードスロット26に対して挿入側端となる。そして、枠体43の一方の側壁前端には、カード本体40の上面、側面、前端面に開口した第1ガイド溝52aが形成され、また、枠体43の他方の側壁前端には、カード本体40の側面および前端面のみに開口した第2ガイド溝52bが形成されている。これらの第1および第2ガイド溝52a、52bは、BT-PCカード20をカードスロット26に

装着する際、B T - P C カード 2 0 の表裏の向きを規制する。

【 0 0 4 2 】

パソコン 1 0 0 に装着される B T - P C カード 2 0 も同様の構成であり、図 1 に示すようにパソコン 1 0 0 の側面部に設けられたカードスロット 1 1 8 を介して装着される。

【 0 0 4 3 】

このような構成の B T - P C カード 2 0 をアクセスポイント 1 0、パソコン 1 0 0 にそれぞれ装着することで、アクセスポイント 1 0 とパソコン 1 0 0 との間で B l u e t o o t h の無線通信規格に従ったデータ通信が可能となる。

【 0 0 4 4 】

ところで、パソコン 1 0 0 がアクセスポイント 1 0 にアクセスする場合に、アクセスポイント 1 0 とパソコン 1 0 0 が初めて接続される状況においては、パソコン 1 0 0 はアクセスポイント 1 0 の P I N コードを入力する必要がある。アクセスポイント 1 0 は、パソコン 1 0 0 から入力された P I N コードが正しければリンクを開設して接続を許可する。このとき、アクセスポイント 1 0 はパソコン 1 0 0 の I D や自身の P I N コードなどを元にリンクキーを作成し、次回パソコン 1 0 0 から接続要求があったときには、このリンクキーによる認証を行うことになる。

【 0 0 4 5 】

アクセスポイント 1 0 の P I N コード（認証パスワード）は予め接続が許可された使用者にのみ知らされているものである。しかし、何らかの手段（例えばコード解読専用のソフトウェアを使用するなどして）で本来の使用者以外の者に知られると、その P I N コードを用いてアクセスポイント 1 0 に不正アクセスして、公衆回線 1 1 を無断で使用する問題がある。

【 0 0 4 6 】

以下では、このような不正アクセスを防止することを主旨として説明する。

【 0 0 4 7 】

図 9 は本発明の無線通信システムの構成を示すブロック図であり、上記図 1 の構成と対応しており、アクセスポイント 1 0 とパソコン 1 0 0 とで無線通信シス

テムを構成してことが示されている。

【0048】

ここで、本実施形態では、図10に示すようにアクセスポイント10の裏面など、目立たないの場所にスライドスイッチ34a、34bが設けられている。これらのスライドスイッチ34a、34bは2位置間を切り換え可能なスイッチであり、禁止モードと許可モードの切り換え操作を行うためのものであり。スライドスイッチ34aはPINコードによる認証動作（新規機器の登録動作）を禁止／許可し、スライドスイッチ34bはセキュリティ情報のメンテナンス動作（PINコードやリンクキーの変更動作）を禁止／許可する。

【0049】

スライドスイッチ34a、34bの操作は基本的にはアクセスポイント10の管理者が行い、通常はスライドスイッチ34a、34b共に禁止状態に設定しておく。そして、アクセスポイント10に新規機器の登録を行う場合に、管理者がスライドスイッチ34aを操作して許可状態に切り換える。

【0050】

このように、本来の使用者が新たに接続を行う場合にスライドスイッチ34aを許可状態に切り換え、普段は禁止状態としておけば、本来の使用者以外の者がアクセスポイント10のPINコードを入力して不正アクセスすることを防止することができる。

【0051】

また、アクセスポイント10のPINコードの変更や、各機器のリンクキーの削除といったモデムアクセスポイント10内に記憶されたセキュリティ情報のメンテナンスは、外部（既に登録されている機器）からコマンドを入力することにより実行できる。このようなセキュリティ情報のメンテナンスをスライドスイッチ34bが許可状態になっているときのみ実行可能とすることで、アクセスポイント10内のセキュリティ情報を勝手にアクセスして変更してしまうことを防止する。

【0052】

なお、スライドスイッチ34a、34bとは別に、図11に示すようなロータ

リスイッチ 3 5 を用いることでも良い。このロータリスイッチ 3 5 は、少なくとも 4 つの位置間を切換え可能なものとし、第 1 の位置で P I N コードによる認証動作（新規機器の登録動作）とセキュリティ情報のメンテナンス動作（P I N コードやリンクキーの変更動作）の両方を禁止し、第 2 の位置で P I N コードによる認証動作のみを許可、第 3 の位置でセキュリティ情報のメンテナンス動作のみを許可、第 4 の位置で P I N コードによる認証動作とセキュリティ情報のメンテナンス動作の両方を許可する。

【 0 0 5 3 】

図 1 2 にスライドスイッチ 3 4 a、3 4 b とロータリスイッチ 3 5 との対応関係を示す。図中の S W 1 はスライドスイッチ 3 4 a、S W 2 はスライドスイッチ 3 4 b を示し、O F F は禁止状態、O N は許可状態を示している。また、1 ～ 4 はロータリスイッチ 3 5 の切換え位置を示している。

【 0 0 5 4 】

このようなスライドスイッチ 3 4 a、3 4 b とロータリスイッチ 3 5 との対応関係を表したテーブルをアクセスポイント 1 0 に持たせておくことで、スライドスイッチ 3 4 a、3 4 b またはロータリスイッチ 3 5 にてアクセスポイント 1 0 の動作状態を切り換えることができる。ただし、ロータリスイッチ 3 5 はスライドスイッチ 3 4 a、3 4 b に比べて操作しづらいため、スライドスイッチ 3 4 a、3 4 b を用いてアクセスポイント 1 0 の動作状態を切り換えることの方が好ましい。以下では、スライドスイッチ 3 4 a、3 4 b を用いてアクセスポイント 1 0 の動作状態を切り換えるものとして説明する。

【 0 0 5 5 】

図 1 3 はアクセスポイント 1 0 と B T - P C カード 2 0 の回路構成を示すブロック図である。

【 0 0 5 6 】

図 1 3 に示すように、アクセスポイント 1 0 は、アクセスポイント全体の動作を制御する C P U 7 2 を備えている。この C P U 7 2 には L E D 2 4、スイッチ群 3 4 a、3 4 b、3 5、P C カードインターフェースとしてのコネクタ 6 0、R O M 7 3、R A M 7 4、不揮発性メモリ 7 5、R T C (R e a l T i m e

C l o c k) 回路 7 6 などが接続される。また、A C アダプタ端子 2 3 から供給される電源は、電源供給部 7 7 を介して C P U 7 2 に供給される。

【 0 0 5 7 】

更に、アクセスポイント 1 0 は、モジュラケーブル 1 2 およびモジュラジャック 3 2 を介して公衆回線 1 1 に接続されるモデム部 7 0 を備えている。このモデム部 7 0 および R S 2 3 2 C コネクタ 2 2 は、切換えスイッチ 7 8 を介して C P U 7 2 に接続されている。なお、モデム部 7 0 およびモジュラジャック 3 0 は送受信部として機能する。

【 0 0 5 8 】

R O M 7 3 は、無線通信および公衆回線 1 1 との通信プロトコル等を格納している。R A M 7 4 は、アクセスポイント 1 0 の動作プログラム、デバイスドライバおよび無線通信プロトコルを含むドライバソフトを格納している。

【 0 0 5 9 】

また、この R A M 7 4 には、ここでは P I N コードの認証動作を制御する第 1 の動作制御情報、セキュリティ情報のメンテナンス動作を制御する第 2 の動作制御情報、基準時刻情報 T M を格納しておくための各種格納部 7 4 a ~ 7 4 c などが設けられている。

【 0 0 6 0 】

不揮発性メモリ 7 5 としては、例えば E E P R O M が用いられる。この不揮発性メモリ 7 5 には、後述するリンクテーブル T 1 および認証エラーテーブル T 2 が設けられていると共に、自身の I D (B T - P C カード 2 0 に登録されている) を保持しておくための I D 格納部 7 5 a や、自身の P I N コード (ユーザが任意に作成した認証用パスワード) を保持しておくためのパスワード格納部 7 5 b などが設けられている。

【 0 0 6 1 】

R T C 回路 7 6 は、現在の時刻を計時するための回路である。

【 0 0 6 2 】

モデム部 7 0 は、B T - P C カード 2 0 から入力されたデジタルデータをアナログデータに変換し、モジュラジャック 3 2 を介して公衆回線 1 1 に転送し、ま

た、モジュラジャック 3 2 を介して公衆回線 1 1 から入力されたアナログデータをデジタルデータに変換し、CPU 7 2 に転送する。

【 0 0 6 3 】

RC 2 3 2 C コネクタ 2 2 は、図示せぬ RS 2 3 2 C ケーブルを介してパソコン 1 0 0 等の外部機器とアクセスポイント 1 0 とをシリアル接続するために設けられている。例えば、RC 2 3 2 C コネクタ 2 2 および RS 2 3 2 C ケーブルを介してアクセスポイント 1 0 に ISDN ターミナルアダプタに接続し、BT-PC カード 2 0 から入力されたデジタルデータをそのまま伝送することも可能である。

【 0 0 6 4 】

切換えスイッチ 7 8 は、モデム部 7 0 およびモジュラジャック 3 2 による公衆回線 1 1 との接続と、RS 2 3 2 C コネクタ 2 2 による他の電子機器との接続とを切り換える。

【 0 0 6 5 】

一方、このアクセスポイント 1 0 に装着される BT-PC カード 2 0 は、BT 規格の無線モジュールとして、アンテナ部 4 6、RF 部 8 0、ベースバンド部 8 1、メモリ 8 2、水晶発振部 8 3、ヘッドセット部 4 8、AD/DA 変換部 8 4、LED 4 7 を備えている。

【 0 0 6 6 】

BT-PC カード 2 0 とアクセスポイント 1 0 とのデータの送受信はコネクタ 4 5 を介して行う。アンテナ部 4 6 は、無線通信を実行するための電波の送信、受信を行い、使用する周波数帯域は BT 規格の 2. 4 ~ 2. 5 GHz となっている。RF 部 8 0 は、使用する所定の無線電波の周波数で通信が実行可能な信号処理を行う。

【 0 0 6 7 】

また、ベースバンド部 8 1 は、アンテナ部 4 6、RF 部 8 0 を介して入力されたデータをデジタル処理し、アクセスポイント 1 0 で処理可能なデータに変換してメモリ 8 2 に格納し、アクセスポイントとの間でデータの授受を行う。なお、ここではメモリ 8 2 に ID が予め記憶されているものとする。実際には、図示せ

ぬ書き換え不可メモリに予めBT-PCカード20に割り付けられたIDが記憶されており、BT-PCカード20装着時にこのBT-PCカード20のIDが機器固有の識別情報として不揮発性メモリ75に書き込まれる。

【0068】

LED47は、例えばデータの送受信時に点灯する。水晶発振部83は、RF部80で使用する基準波を供給する。ヘッドセット部48は、ヘッドフォンとマイクロフォンとを有するヘッドセットを接続し、音声信号の入出力を行う。また、AD/DA変換部84は、ヘッドセット部48から入力されたアナログの音声信号をデジタルデータに変換すると共に、アクセスポイント10からベースバンド部81を介して入力されたデジタルの音声信号をアナログデータに変換してヘッドセット部48に出力する。

【0069】

図14はである。アクセスポイント10に外部機器として接続されるパソコン100とBT-PCカード20の回路構成を示すブロック図。

【0070】

パソコン100には、図1に示すようにキーボード112が設けられた本体114と、この本体114に開閉自在に設けられた液晶表示パネル116とを有している。本体114にはカードスロット118が設けられ、このカードスロット118にはBT-PCカード20が脱着自在に装着されている。カードスロット118の構成は上述したアクセスポイント10のカードスロット26とほぼ同一である。また、BT-PCカード20はアクセスポイント10と共通であり、その内部構成は図13と同様であるため、ここではその説明を省略する。

【0071】

また、パソコン100には、BT-PCカード20との間でデータの送受信を行うPCMCIA規格のインターフェースコネクタ120と、パソコン全体の動作を制御するCPU122を備えている。CPU122には、USB124、ROM126、RAM128などが接続されている。

【0072】

USB124は、例えばアクセスポイント10とRS232Cコネクタ22を

介してシリアル接続する際に使用する。ROM 1 2 6 には、プログラム等のデータが記憶されている。RAM 1 2 8 には、CPU 1 2 2 の処理動作に必要な各種のデータが記憶される。また、このRAM 1 2 8 には、パソコン 1 0 0 に設定されたPINコード（ユーザが任意に作成した認証パスワード）や、BT-PCカード 2 0 から読み込んだIDを格納したおくための各種データ格納部が設けられている。

【0 0 7 3】

次に、アクセスポイント 1 0 が管理しているリンクテーブル T 1 および認証エラーテーブル T 2 の構成について説明する。

【0 0 7 4】

図 1 5 はリンクテーブル T 1 の構成を示す図である。

【0 0 7 5】

リンクテーブル T 1 には、各機器に固有のID（アドレス）、そのIDなどを元に作成されたリンクキー、最終接続時刻、データ有無フラグが登録される。

【0 0 7 6】

上述したように、アクセスポイント 1 0 では、新たな機器（リンクテーブル T 1 に未登録の機器）から接続要求があったときにはPINコードによる認証を行い、認証OKの場合にその機器のIDなどを元にリンクキーを作成し、そのリンクキーをIDと共にリンクテーブル T 1 に登録する。また、このときの接続時刻をRTC回路 7 6 から取得してリンクテーブル T 1 に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【0 0 7 7】

図 1 6 は認証エラーテーブル T 2 の構成を示す図である。

【0 0 7 8】

認証エラーテーブル T 2 は、各機器に固有のID（アドレス）、認証エラー回数、最終接続時刻、データ有無フラグが登録される。

【0 0 7 9】

アクセスポイント 1 0 は、PINコードによる認証の際に認証エラーと判定さ

れた機器に対し、その機器の I D と認証エラー回数とを対応付けて認証エラーテーブル T 2 に登録しておく。認証エラー回数の初期値は「1」であり、機器が認証エラーと判定される毎に更新される。また、このときの接続時刻を R T C 回路 7 6 から取得して認証エラーテーブル T 2 に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【 0 0 8 0 】

リンクテーブル T 1 及び認証エラーテーブル T 2 の登録数は不揮発性メモリ 7 5 の容量に応じて決められており、図 1 5 の例ではリンクテーブル T 1 の最大登録件数は N 件、図 1 6 の例では認証エラーテーブル T 2 の最大登録件数は M 件である。

【 0 0 8 1 】

次に、本システムの動作について説明する。

【 0 0 8 2 】

ここでは、アクセスポイント 1 0 に対する不正アクセスを防止するための処理として、(a) スイッチによる動作状態の切り換え処理、(b) 外部機器との接続処理、(c) セキュリティ情報のメンテナンス処理、(d) 接続時の認証エラー処理に分けて説明する。

【 0 0 8 3 】

(a) スイッチによる動作状態の切り換え処理

上述したように、アクセスポイント 1 0 の裏面には、アクセスポイント 1 0 の動作状態を切替えるためのスライドスイッチ 3 4 a、3 4 b が設けられている。スライドスイッチ 3 4 a は P I N コードによる認証動作を禁止状態または許可状態とするものであり、スライドスイッチ 3 4 b はセキュリティ情報のメンテナンス動作を禁止状態または許可状態とするものである。

【 0 0 8 4 】

ここで、スライドスイッチ 3 4 a による動作状態の切替え処理について説明する。

【 0 0 8 5 】

図17はアクセスポイント10に設けられたスライドスイッチ34aによる動作状態の切換え処理を示すフローチャートである。なお、図17はアクセスポイント10のCPU72が実行するプログラムの処理を示したものである。また、図中SW1はスライドスイッチ34aのことである。

【0086】

アクセスポイント10では、スライドスイッチ34aの状態を常に監視している。アクセスポイント10は、スライドスイッチ34aが禁止状態から許可状態に切り換えられたことを検知すると（ステップA11のYes）、まず、図13に示すRTC回路76から現在時刻を取得し、この時刻を基準時刻情報TMとしてRAM74内の基準時刻格納部74cにセットする（ステップA12）。そして、PINコードの認証動作を許可とする第1の動作制御情報をRAM74内の第1の動作制御情報格納部74aにセットする（ステップA13）。

【0087】

一方、アクセスポイント10は、スライドスイッチ34aが許可状態から禁止状態に切り換えられたことを検知すると（ステップA14のYes）、PINコードの認証動作を禁止とする第1の動作制御情報をRAM74内の第1の動作制御情報格納部74aにセットする（ステップA15）。

【0088】

また、スライドスイッチ34aが禁止状態から許可状態に切り換えられた後に、その切り換え時にセットされた基準時刻情報TMと現在時刻との差が所定時間以上になると、つまり、スライドスイッチ34aが許可状態に切り換えられてから所定時間経過すると（ステップA16のYes）、アクセスポイント10は、スライドスイッチ34aの状態に関係なく、PINコードの認証動作を禁止とする第1の動作制御情報を第1の動作制御情報格納部74aにセットする（ステップA17）。

【0089】

スライドスイッチ34bについても同様である。

【0090】

すなわち、スライドスイッチ34bが禁止状態から許可状態に切り換えられる

と、そのときの時刻が基準時刻情報TMとしてRAM 7 4 内の基準時刻格納部 7 4 c にセットされると共に、セキュリティ情報のメンテナンス動作を許可とする第 2 の動作制御情報がRAM 7 4 内の第 2 の動作制御情報格納部 7 4 b にセットされる。一方、スライドスイッチ 3 4 b が許可状態から禁止状態に切り換えられると、セキュリティ情報のメンテナンス動作を禁止とする第 2 の動作制御情報がRAM 7 4 内の第 2 の動作制御情報格納部 7 4 b にセットされる。

【 0 0 9 1 】

更に、スライドスイッチ 3 4 b が禁止状態から許可状態に切り換えられた後、その切り換え時にセットされた基準時刻情報TM（スライドスイッチ 3 4 a を管理するものとは別のものとする）と現在時刻との差が所定時間以上になると、つまり、スライドスイッチ 3 4 b が許可状態に切り換えられてから所定時間経過すると、スライドスイッチ 3 4 b の状態に関係なく、セキュリティ情報のメンテナンス動作を禁止とする第 2 の動作制御情報がRAM 7 4 内の第 2 の動作制御情報格納部 7 4 b にセットされる。

【 0 0 9 2 】

なお、上記所定時間は例えば 1 0 分程度が妥当であるが、その時間は予め決められていても良いし、アクセスポイント 1 0 の管理者が任意に設定できるようにしても良い。

【 0 0 9 3 】

(b) 外部機器との接続処理

次に、外部機器との接続処理について説明する。

【 0 0 9 4 】

図 1 8 はアクセスポイント 1 0 における外部機器との接続処理の動作を示すフローチャートである。なお、図 1 8 はアクセスポイント 1 0 のCPU 7 2 が実行するプログラムの処理を示したものである。

【 0 0 9 5 】

例えば外部機器であるパソコン 1 0 0 からアクセスポイント 1 0 に対して、無線通信により接続要求が送られてくると、アクセスポイント 1 0 は、まず、RAM 7 4 内の第 1 の動作制御情報格納部 7 4 a に格納された第 1 の動作制御情報に

基づいて、P I Nコードによる認証動作が許可されているか否かをチェックする（ステップB 1 1）。

【0 0 9 6】

上述したように、スライドスイッチ3 4 aが許可状態に切り換えられており、かつ、スライドスイッチ3 4 aが許可状態に切り換えられてから所定時間経過していない場合に、第1の動作制御情報は許可を示している。また、スライドスイッチ3 4 aが禁止状態に切り換えられているか、あるいは、スライドスイッチ3 4 aが許可状態に切り換えられてから所定時間経過している場合に、第1の動作制御情報は禁止を示している。

【0 0 9 7】

P I Nコードによる認証動作が許可されていれば（ステップB 1 2のY e s）、アクセスポイント1 0は接続要求先のパソコン1 0 0が初めての接続か否かをパソコン1 0 0に対するリンクキーの有無によってチェックする（ステップB 1 3）。すなわち、アクセスポイント1 0が持つリンクテーブルT 1には、これまでにアクセスポイント1 0に接続された機器のI Dとリンクキーとが登録されている。このリンクテーブルT 1にパソコン1 0 0に対するリンクキーがなければ、言い換えれば、リンクテーブルT 1にパソコン1 0 0のI Dが登録されていなければ、パソコン1 0 0は初めての接続と判定される。

【0 0 9 8】

ここで、アクセスポイント1 0とパソコン1 0 0とが初めて接続される状況においては（ステップB 1 3のY e s）、パソコン1 0 0からアクセスポイント1 0のP I Nコードを入力する必要がある。

【0 0 9 9】

パソコン1 0 0からP I Nコードが入力されると、アクセスポイント1 0はこのP I Nコードによる認証を行う（ステップB 1 4）。上記P I Nコードが正しい場合つまり不揮発性メモリ7 5内のパスワード格納部7 5 bに格納された自身のP I Nコードと一致した場合には認証可と判定する（ステップB 1 5のY e s）。

【0 1 0 0】

ここで、PINコードによる認証動作について、図22を参照して具体的に説明する。

【0101】

今、機器Aが機器Bに接続を行う場合を想定する。本実施形態では、機器Aはパソコン100、機器Bはアクセスポイント10に相当する。また、図中のパスワードとは、アクセスポイント10のPINコードのことである。

【0102】

図22に示すように、まず、機器Aがコネクション要求（接続要求）を送信する（ステップS1）。機器Bは機器Aからのコネクション要求を受信すると、この受信データを解析し、問題がない場合にはコネクション確立のメッセージを機器Aに送信し（ステップS2）、しかる後に、機器A-B間でコネクションが確立する（ステップS3）。なお、この場合のコネクションとは、通信の低位レイヤのコネクションを意味するもので、例えば「仮のネットワークアドレスが与えられた」という状況を意味するものとし、必ずしも上位アプリケーションのサービスを意味するものではない。

【0103】

上記コネクションが確立した後、パスワードによる認証手続きが行なわれる。すなわち、機器Bは、上記コネクションが確立すると、機器Aに認証要求を出力し、パスワードの入力を促す（ステップS4）。これにより、機器Aのユーザは機器Bのパスワードを入力し、それを送信する（ステップS5）。

【0104】

上記パスワードを受信した機器Bは、自機のパスワードと受信したパスワードとを照合する。照合結果が間違っていれば、パスワードが違う旨のメッセージを機器Aに返すが、照合結果に問題がなければ認証を完了する（ステップS6）。

【0105】

図18に戻って、上記のようなPINコードによる認証動作が行われた結果、認証可と判定された場合に（ステップB15のYes）、アクセスポイント10はリンクを開設し（ステップB16）、パソコン100に対するリンクキーを作成する（ステップB17）。詳しくは、パソコン100のIDを取得し、そのI

Dと自身のPINコードなどをアクセスポイント10側で発生する乱数を掛け合わせるなどして、解読困難なリンクキーを作成する。そして、アクセスポイント10は上記作成されたリンクキーをパソコン100のIDと共にリンクテーブルT1に登録する（ステップB18）。その際、RTC回路76から現在の時刻を取得し、そのときの時刻を最終接続時刻としてリンクテーブルT1に登録すると共に、データ有無フラグを「有」にセットしておく。

【0106】

ここで、リンクテーブルT1に新たな機器のデータを登録する際に、リンクテーブルT1に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータをリンクテーブルT1から削除して、そこに新たな機器のデータを登録するものとする。このように、接続される可能性の低い機器のリンクキーの代わりに新たに接続された機器のリンクキーを登録することで、不揮発性メモリ75に設けられるリンクテーブルT1の登録件数（図15の例ではN件）の中で新たな接続相手を優先してPINコードを効率的に管理でき、使い勝手を向上させることができる。

【0107】

なお、例えば各機器の本機器に対するアクセス回数をリンクテーブルT1に記憶させておき、アクセス回数の最も少ない機器のデータを削除することでも良い。

【0108】

また、各機器のリンクテーブルT1への登録時刻をリンクテーブルT1に記憶させておき、その登録時刻の最も古い機器のデータを削除することでも良い。

【0109】

PINコードによる認証がOKとされると、アクセスポイント10とパソコン100との接続が確立され、互いに無線によるデータ通信が可能となる（ステップB19）。また、PINコードによる認証がNGであった場合には（ステップB15のNo）、アクセスポイント10はそのときの接続要求先であるパソコン100との接続を拒否する。

【0110】

一方、PINコードによる認証動作が禁止されている場合（ステップB12のNo）あるいはパソコン100が以前にアクセスポイント10に接続されたことがある場合には（ステップB13のNo）、アクセスポイント10はリンクキーによる認証を行う（ステップB20）。この場合、接続要求先のパソコン100が以前にアクセスポイント10に接続されたことがあれば、パソコン100に対するリンクキーがリンクテーブルT1に登録されているので、そのリンクキーを用いて認証を行うことができる。認証OKであれば（ステップB21のYes）、アクセスポイント10はパソコン100との接続を確立する（ステップB19）。また、PINコードによる認証がNGであった場合には（ステップB21のNo）、アクセスポイント10はそのときの接続要求先であるパソコン100との接続を拒否する。

【0111】

このように、PINコードによる認証動作が許可されている場合のみ、新たな機器がアクセスポイント10へのアクセスを試みることができる。したがって、普段はスライドスイッチ34aの操作によりPINコードによる認証動作を禁止しておけば、本来の利用者以外の者がアクセスポイント10のPINコードを何らかの手段で入手したとしても、アクセスポイント10に対してアクセスすることはできないため、公衆回線11が無断で使用するなどの不正行為を防ぐことができる。

【0112】

また、アクセスポイント10の管理者がスライドスイッチ34aを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ34aの状態に関係なく、PINコードによる認証動作が自動的に禁止されるため、アクセスポイント10のセキュリティを強化することができる。

【0113】

（c）セキュリティ情報のメンテナンス処理

次に、セキュリティ情報のメンテナンス処理について説明する。

【0114】

図19はアクセスポイント10におけるセキュリティ情報のメンテナンス処理

の動作を示すフローチャートである。なお、図19はアクセスポイント10のCPU72が実行するプログラムの処理を示したものである。

【0115】

今、外部機器であるパソコン100との接続が確立された状態で（ステップC11）、パソコン100からセキュリティ情報のメンテナンスコマンドが無線より送信されたものとする。セキュリティ情報のメンテナンスコマンドには、PINコードの読み出しや書き換え、リンクテーブルT1の読み出しや削除などがある。

【0116】

アクセスポイント10は上記メンテナンスコマンドを受信すると、まず、RAM74内の第2の動作制御情報格納部74bに格納された第2の動作制御情報に基づいて、セキュリティ情報のメンテナンス動作が許可されているか否かをチェックする（ステップC12）。

【0117】

上述したように、スライドスイッチ34bが許可状態に切り換えられており、かつ、スライドスイッチ34bが許可状態に切り換えられてから所定時間経過していない場合に、第2の動作制御情報は許可を示している。また、スライドスイッチ34bが禁止状態に切り換えられているか、あるいは、スライドスイッチ34bが許可状態に切り換えられてから所定時間経過している場合に、第2動作制御情報は禁止を示している。

【0118】

セキュリティ情報のメンテナンス動作が禁止されていれば（ステップC13のNo）、アクセスポイント10は上記メンテナンスコマンドを拒否する（ステップC14）。これにより、どのような外部機器であっても、セキュリティ情報のメンテナンスを行うことはできない。

【0119】

一方、セキュリティ情報のメンテナンス動作が許可されていれば（ステップC13のYes）、アクセスポイント10は上記メンテナンスコマンドを実行する（ステップC15）。その際、PINコードの書き換えが行われた場合には（ス

テップC16のYes)、アクセスポイント10はリンクテーブルT1のデータをすべて削除する(ステップC17)。

【0120】

このように、セキュリティ情報のメンテナンス動作が許可されている場合のみ、外部機器からコマンドを送って、PINコードの書き換え等を行うことができる。したがって、普段はスライドスイッチ34bの操作によりセキュリティ情報のメンテナンス動作を禁止しておけば、勝手にセキュリティ情報をアクセスすることはできないため、アクセスポイント10のセキュリティを確保できる。

【0121】

また、アクセスポイント10の管理者がスライドスイッチ34bを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ34bの状態に関係なく、セキュリティ情報のメンテナンス動作が自動的に禁止されるため、アクセスポイント10のセキュリティを確保することができる。

【0122】

さらに、PINコードが変更された場合には不正アクセス者によるデータの改竄の可能性を考慮してリンクテーブルT1のデータをすべてクリアしておくことで、セキュリティをさらに強化することができる。リンクテーブルT1をクリアした場合には、すべての外部機器に対して再度PINコードの入力を求めることになる。この場合、アクセスポイント10で新たに設定されたPINコードを知らないユーザはアクセスポイント10へ接続することはできないことになる。

【0123】

(d) 接続時の認証エラー処理

次に、接続時の認証エラー処理について説明する。

【0124】

図20および図21はアクセスポイント10における接続時の認証エラー処理の動作を示すフローチャートである。なお、図20および図21はアクセスポイント10のCPU72が実行するプログラムの処理を示したものである。

【0125】

今、外部機器であるパソコン100のIDがリンクテーブルT1に登録されて

いないものとする。このパソコン 1 0 0 から接続要求があると（ステップ D 1 1）、アクセスポイント 1 0 は認証エラーテーブル T 2 を参照する（ステップ D 1 2）。認証エラーテーブル T 2 には、図 1 6 に示すように、以前に認証エラーとなった機器の I D 等が登録されている。

【 0 1 2 6 】

この認証エラーテーブル T 2 にパソコン 1 0 0 の I D が登録されていなかった場合には（ステップ D 1 3 の N o ）、アクセスポイント 1 0 は通常通り P I N コードによる認証を行う（ステップ D 1 4）。そして、認証 O K であれば、つまり、パソコン 1 0 0 が入力した P I N コードがアクセスポイント 1 0 の P I N コードと一致すれば（ステップ D 1 5 の Y e s ）、アクセスポイント 1 0 はパソコン 1 0 0 の接続を許可する（ステップ D 1 6）。

【 0 1 2 7 】

一方、認証エラーであった場合、つまり、パソコン 1 0 0 が入力した P I N コードがアクセスポイント 1 0 の P I N コードと一致しなかった場合には（ステップ D 1 5 の N o ）、アクセスポイント 1 0 はパソコン 1 0 0 の接続を拒否する（ステップ D 1 7）。その際、アクセスポイント 1 0 はパソコン 1 0 0 の I D を取得し、その I D を認証エラーテーブル T 2 に登録すると共に、上記 I D に対応したエラー回数を初期値“1”とし、さらに、R T C 回路 7 6 から現在の時刻を取得して、その時刻を最終接続時刻として登録する（ステップ D 1 8）。

【 0 1 2 8 】

また、上記ステップ D 1 3 において、リンクテーブル T 1 に接続要求先のパソコン 1 0 0 の I D が登録されていたとする。つまり、以前にパソコン 1 0 0 から入力された P I N コードが正しくないとして拒否されていたとする。

【 0 1 2 9 】

このような場合において、アクセスポイント 1 0 は、まず、認証エラーテーブル T 2 内のパソコン 1 0 0 の I D に対応したエラー回数が所定回数を越えているか否かをチェックする（ステップ D 1 9）。その結果、エラー回数が所定回数以内であれば（ステップ D 1 9 の N o ）、アクセスポイント 1 0 は通常通り P I N コードによる認証を行う（ステップ D 2 0）。そして、認証 O K であれば、つま

り、パソコン100が入力したPINコードがアクセスポイント10のPINコードと一致すれば（ステップD21のYes）、アクセスポイント10はパソコン100の接続を許可する（ステップD22）。このとき、認証エラーテーブルT2からパソコン100に関するデータを削除しておく（ステップD23）。

【0130】

一方、エラー回数が所定回数を越えている場合には（ステップD19のNo）、パソコン100は不正アクセス者であると判断し、パソコン100の接続を拒否する（ステップD24）。その際、認証エラーテーブルT2内の当該パソコン100のエラー回数を更新すると共に、RTC回路76から現在の時刻を取得して最終接続時刻として更新する（ステップD25）。また、上記ステップD21において認証エラーとなった場合にも同様にであり、接続の拒否と共に認証エラーテーブルT2内の当該パソコン100に関するデータの更新を行う（ステップD24、D25）。

【0131】

このように、PINコードによる認証時に認証エラーとなった場合の回数をカウントしておき、同一機器の認証エラー回数が所定回数を超えた場合には当該機器の接続を完全に拒否することで、同じ機器が何度もPINコードを入力してアクセスポイント10に不正にアクセスすることを防止して、アクセスポイント10のセキュリティを強化することができる。

【0132】

なお、上記所定回数は例えば5回程度が妥当であるが、その回数は予め決められていても良いし、アクセスポイント10の管理者が任意に設定できるようにしても良い。

【0133】

また、認証エラーテーブルT2に新たな機器のデータを登録する際に、認証エラーテーブルT2に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータを認証エラーテーブルT2から削除して、そこに新たな機器のデータを登録する。このように、古いデータを削除することで、不揮発性メモリ75に設けられる認証エラーテーブルT2の登録件数（図16

の例ではM件)の中で新たな接続相手を優先して認証エラー回数を効率的に管理でき、使い勝手を向上させることができる。

【0134】

以上のように、アクセスポイント10に設けられたスイッチの操作によりPINコードによる認証動作やセキュリティ情報のメンテナンス動作を禁止することで、外部からの不正なアクセスを防止してセキュリティを強化することができる。さらに、スイッチの状態に関係なく、所定時間経過後にはPINコードによる認証動作やセキュリティ情報のメンテナンス動作を自動的に禁止状態に切り換えることで、管理者がスイッチ操作を忘れたとしてもセキュリティを確保することができる。

【0135】

また、同じ機器から不正なPINコードの入力が何度もあった場合に、以後、その機器の接続を完全に拒否することで、正しいPINコードを知らない者が不正アクセスを試みることを防止することができる。

【0136】

また、不揮発性メモリ75に設けられるリンクテーブルT1へのリンクキーの登録件数数が記憶可能な最大数に達した後、新たな接続相手とリンクキーを登録する場合には、一定の規則(接続時刻が古いものやアクセス頻度が低いものなど)に従って既に記憶されたリンクキーを削除してその領域に新たなリンクキーを登録することで、新たな接続相手を優先して、その以後の接続時におけるPINコード入力を不要にでき、使い勝手を向上させることができる。

【0137】

また、アクセスポイント10内のPINコードが変更された場合に、リンクテーブルT1に登録されている各機器のリンクキーのすべてを削除して、接続時に新たなPINコードの入力を要求するようにしたことで、セキュリティを強化することができる。

【0138】

ところで、各機器に装着されるBT-PCカード20にはBTモジュールのIDが登録されており、アクセスポイント10にBT-PCカード20が装着され

た場合、図15に示すCPU72はBT-PCカード20に登録されているIDを機器固有の情報として、アクセスポイント10内の不揮発性メモリ75のID格納部75aに格納する。

【0139】

ここで、CPU72がPCカードインターフェースとしてのコネクタ60を介してBT-PCカード20が交換されたことを検知した場合、リンクテーブルT1のデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【0140】

これは、BTモジュール（IDを記憶している）がPCカードなどの交換可能なユニットで構成されていた場合に、ユーザの手違いで最初にアクセスポイント10に装着されていたBTモジュールとは別のBTモジュールが装着される可能性があるためである。つまり、リンクキーはIDなどを元に作成されるものであるため、BTモジュール交換前のIDで作成されたリンクキーをそのまま残しておく、BTモジュール交換後のIDによって作成されるリンクキーとの矛盾が生じ、外部機器との接続ができなくなる。このような不具合を解消するため、BTモジュールが交換された場合には、現在リンクテーブルT1に登録されているデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【0141】

なお、本発明は、アクセスポイント10から離れた場所にある外部機器から無線により不正アクセスする場合に特に有効であるが、アクセスポイント10へのアクセス手段として必ずしも無線である必要はない。すなわち、例えば図1に示すアクセスポイント10とパソコン100とが通信ケーブルを介して接続されるようなシステムであっても、上記実施形態で同様の手法を適用することで不正アクセスを防止することができる。

【0142】

また、上記実施形態では、公衆回線11の接続機能を備えたアクセスポイント10を例にして説明したが、無線等により他機器との接続を行うための通信機能

を備えた機器であれば、そのすべての機器に本発明の手法を適用できるものである。

【0143】

また、各機器に用いられる無線通信モジュールとしては、PCカード等の交換可能なユニットで構成されている必要はなく、機器内に内蔵されているものであっても良い。

【0144】

また、無線通信方式としては、Bluetoothに限らず、他の方式であっても良い。

【0145】

要するに、本発明は上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態で示される全構成要件から幾つかの構成要件が削除されても、「発明が解決しようとする課題」で述べた効果が解決でき、「発明の効果」の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【0146】

また、上述した実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリなどの記録媒体に書き込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【0147】

【発明の効果】

以上詳記したように本発明によれば、スイッチの状態に応じて、特定の識別コードによる認証が禁止または許可される。したがって、上記特定の識別コードを

不正に知り得たとしても、上記スイッチを直接に設定操作しない限り、本機器とのリンクを張ることができない。さらに、所定時間経過後は上記特定の識別コードによる認証が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【0148】

また、他の機器との間で接続を行うための各種管理情報に対する変更操作がスイッチの状態によって禁止または許可される。したがって、他の機器の不正ユーザが本機器と接続できたとしても、上記スイッチを直接に設定操作しない限り、各種管理情報を勝手に変更することはできない。さらに、所定時間経過後は上記各種管理情報の変更が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【0149】

また、所定回数を越えて認証エラーとなった機器からの接続要求が拒否されるため、同一機器からの不正な接続の試みを防止できる。

【0150】

また、メモリの登録件数が一杯にある状態では、その中で接続の可能性の低いリンク情報が削除されて新たな機器のリンク情報が登録されるため、使い勝手を向上させることができる。

【0151】

また、特定の識別コードが変更された場合にメモリ内のすべてのリンク情報が削除されるので、新たな識別コードを知らないユーザからの不正アクセスを防止できる。

【0152】

また、交換可能な無線通信ユニットを備えた電子機器において、無線通信ユニットの交換があった場合に、メモリ内のすべてのリンク情報が削除されるので、交換前の無線通信ユニットの識別コードにより作成されたリンク情報と交換後の無線通信ユニットの識別コードにより作成されたリンク情報との矛盾をなくして、他の機器との接続ができなくなることを防止できる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図。

【図 2】

上記無線通信システムに用いられるアクセスポイントの分解斜視図。

【図 3】

上記アクセスポイントを縦置きで使用した状態を示す斜視図。

【図 4】

上記アクセスポイントの背面側を示す斜視図。

【図 5】

上記アクセスポイントを横置きで使用した状態を示す斜視図。

【図 6】

上記アクセスポイントの底面側を示す斜視図。

【図 7】

上記アクセスポイントに装着される B T - P C カードの斜視図。

【図 8】

上記 B T - P C カードの分解斜視図。

【図 9】

上記無線通信システムの構成を示すブロック図。

【図 1 0】

上記アクセスポイントに設けられたスライドスイッチの構成を示す図。

【図 1 1】

上記アクセスポイントに設けられたロータリスイッチの構成を示す図。

【図 1 2】

上記スライドスイッチと上記ロータリスイッチとの対応関係を示す図。

【図 1 3】

上記アクセスポイントと B T - P C カードの回路構成を示すブロック図。

【図 1 4】

上記アクセスポイントに外部機器として接続されるパソコンと B T - P C カードの回路構成を示すブロック図。

【図 1 5】

上記アクセスポイントに設けられたリンクテーブルの構成を示す図。

【図 1 6】

上記アクセスポイントに設けられた認証エラーテーブルの構成を示す図。

【図 1 7】

上記アクセスポイントに設けられたスライドスイッチによる動作状態の切換え処理を示すフローチャート。

【図 1 8】

上記アクセスポイントにおける外部機器との接続処理の動作を示すフローチャート。

【図 1 9】

上記アクセスポイントにおけるセキュリティ情報のメンテナンス処理の動作を示すフローチャート。

【図 2 0】

上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。

【図 2 1】

上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。

【図 2 2】

P I Nコードによる認証動作を説明するための図。

【符号の説明】

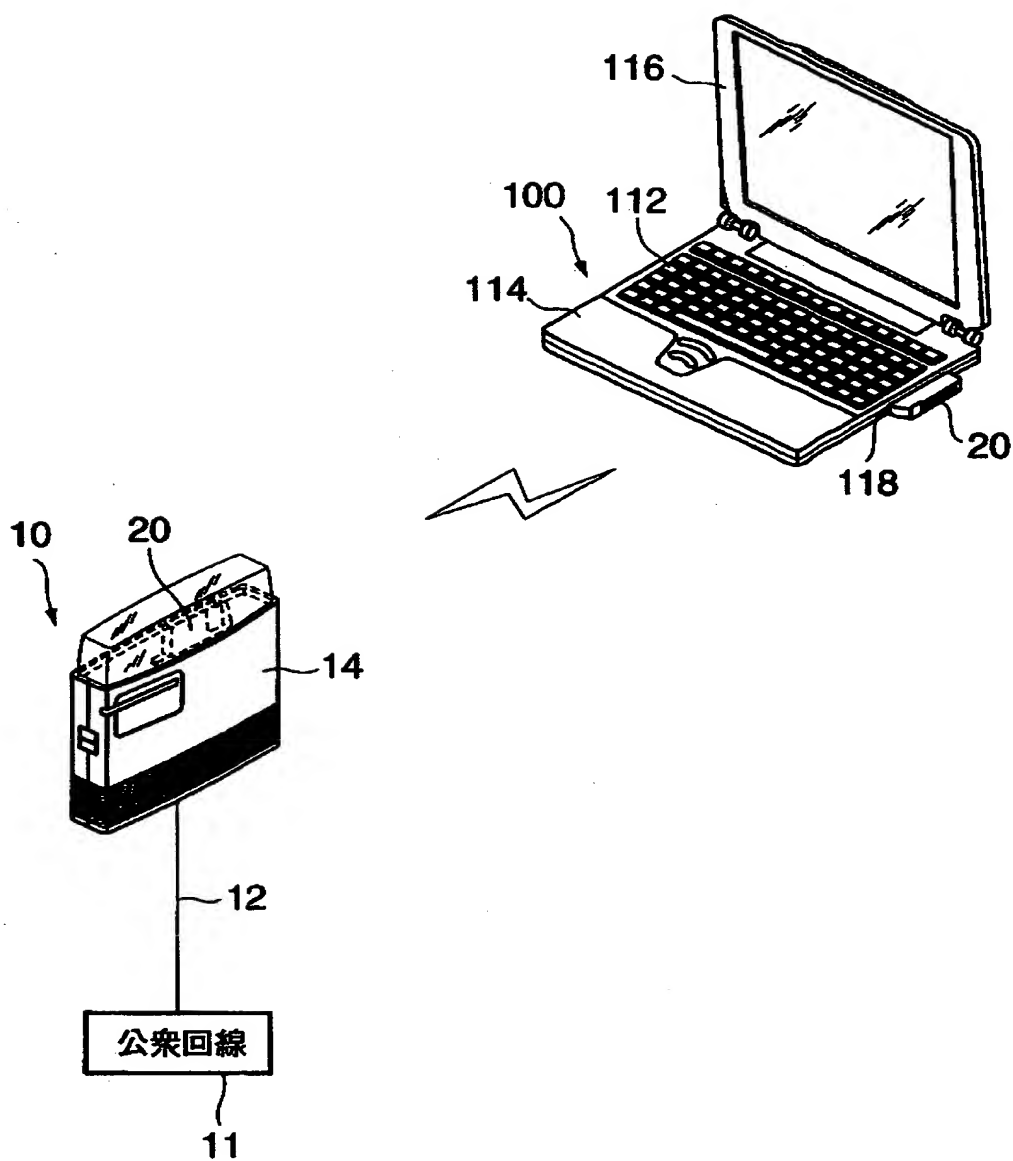
- 1 0 … アクセスポイント
- 1 2 … モジュラケーブル
- 1 4 … 機器本体
- 2 0 … B T - P C カード
- 3 4 a、3 4 b … スライドスイッチ
- 3 5 … ロータリスイッチ
- 4 0 … カード本体

4 2 …送受信部
4 6 …アンテナ部
4 5、6 0 …コネクタ
7 0 …モデム部
7 2 …C P U
7 4 …R A M
7 4 a …第 1 の動作制御情報格納部
7 4 b …第 2 の動作制御情報格納部
7 4 c …基準時刻格納部
7 5 …不揮発性メモリ
7 5 a …I D 格納部
7 5 b …パスワード格納部
T 1 …リンクテーブル
T 2 …認証エラーテーブル
7 6 …R T C 回路
1 0 0 …パソコン
1 1 2 …キーボード
1 1 6 …L C D パネル
1 2 0 …インターフェースコネクタ
1 2 2 …C P U

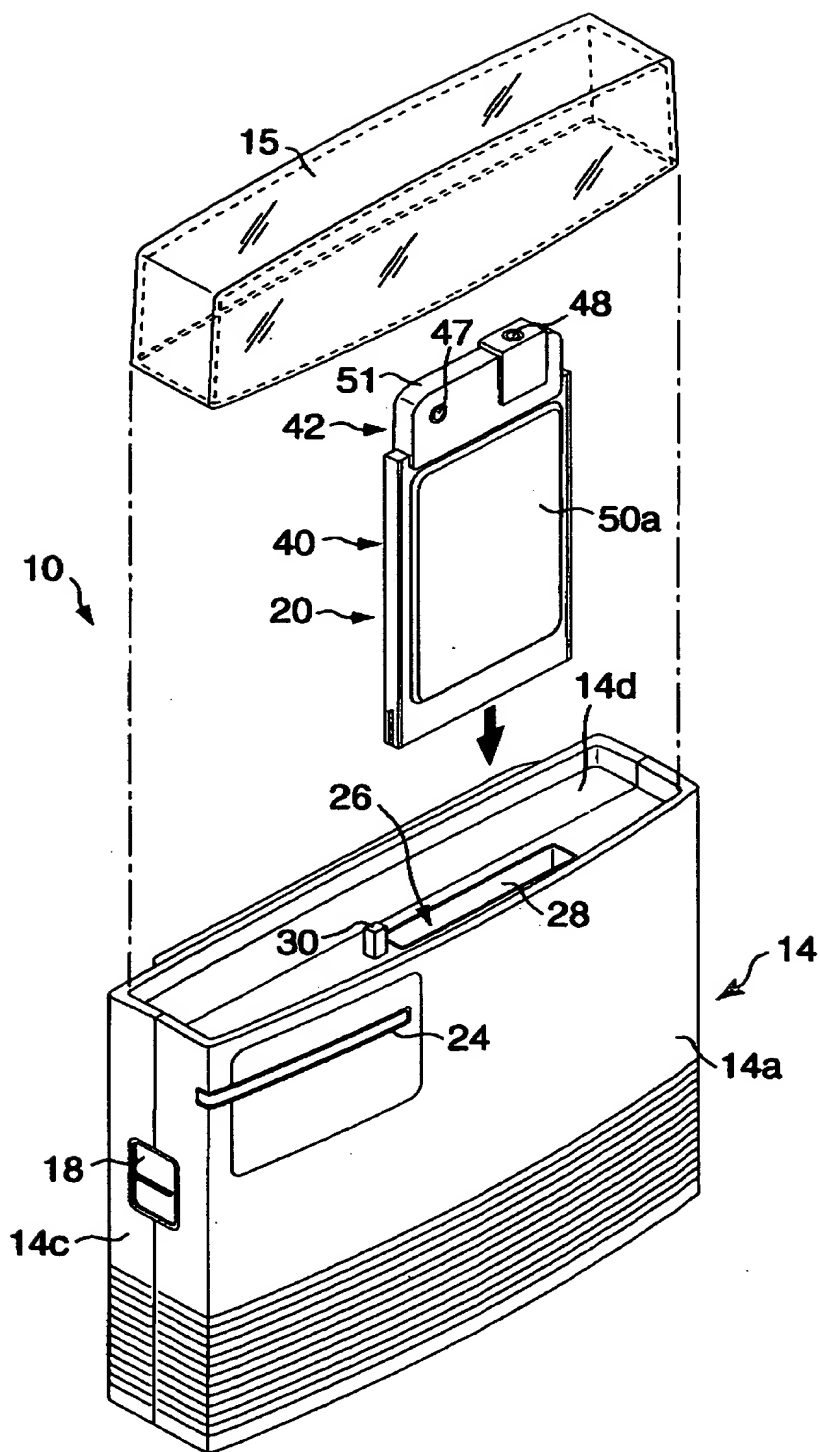
【書類名】

図面

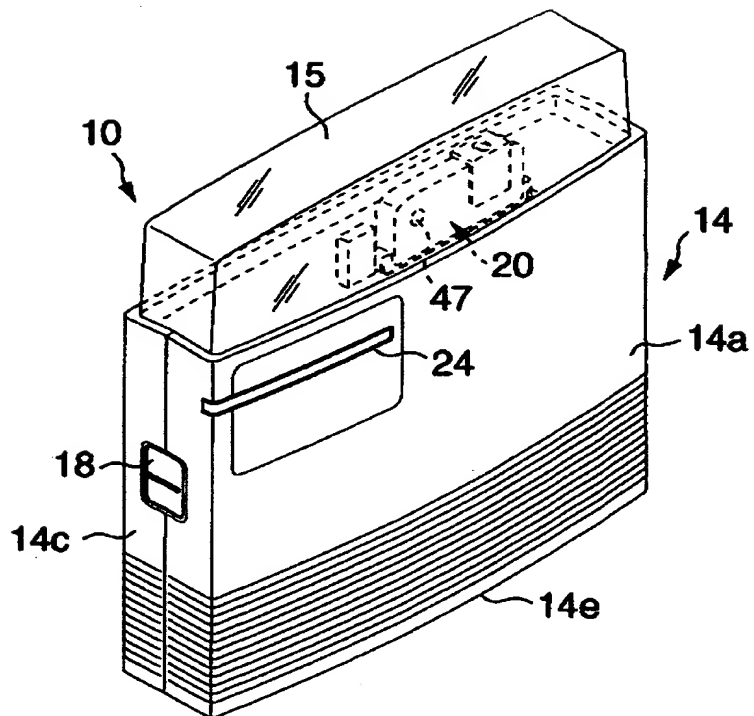
【図 1】



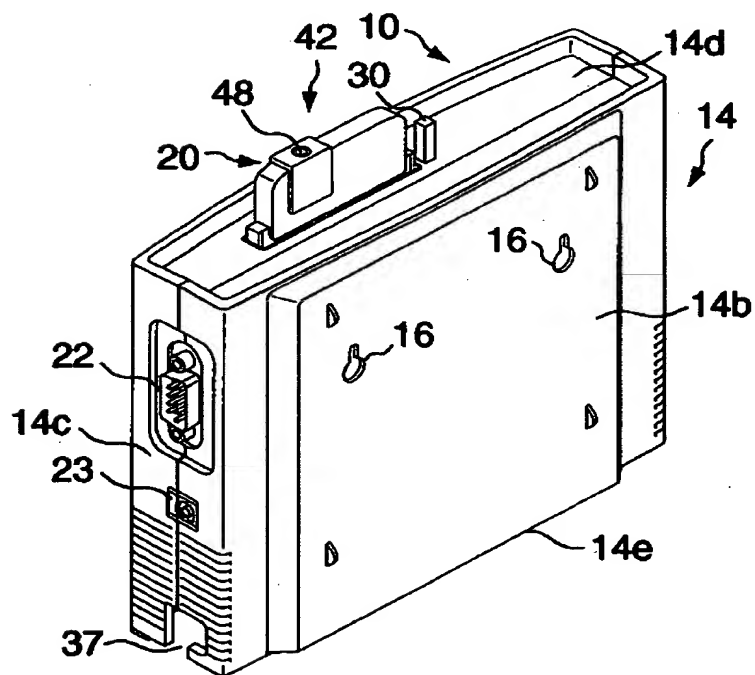
【図 2】



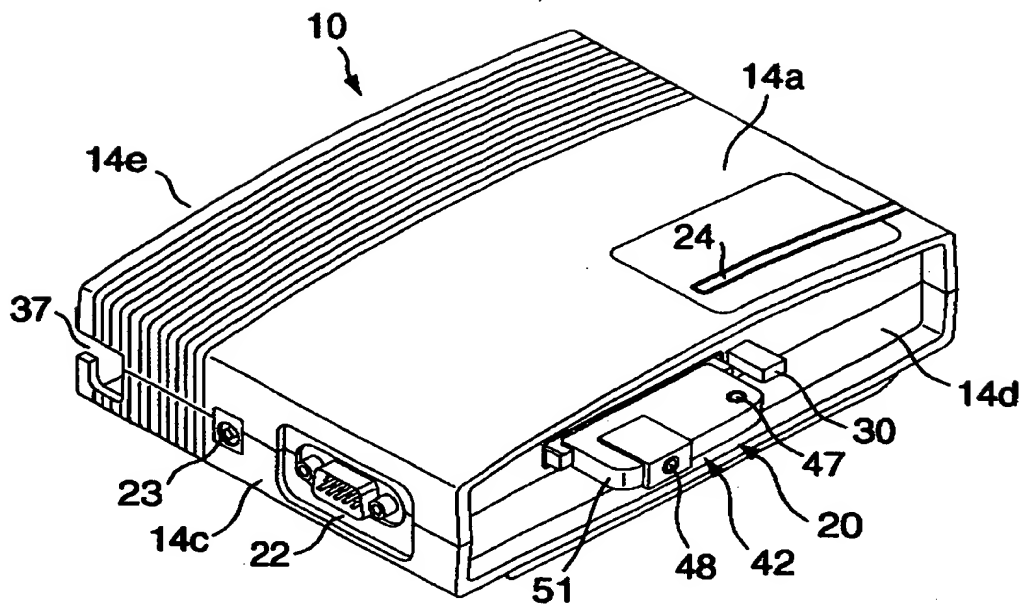
【図 3】



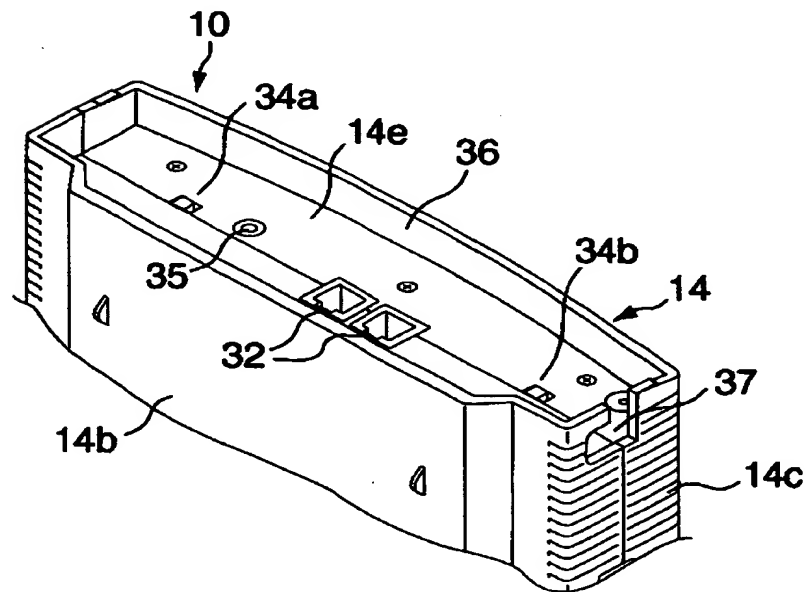
【図 4】



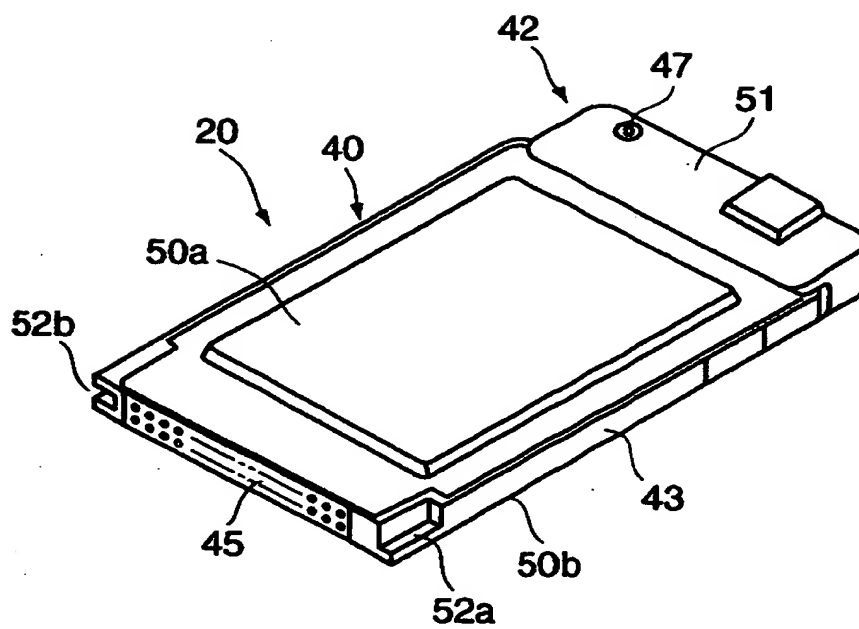
【図 5】



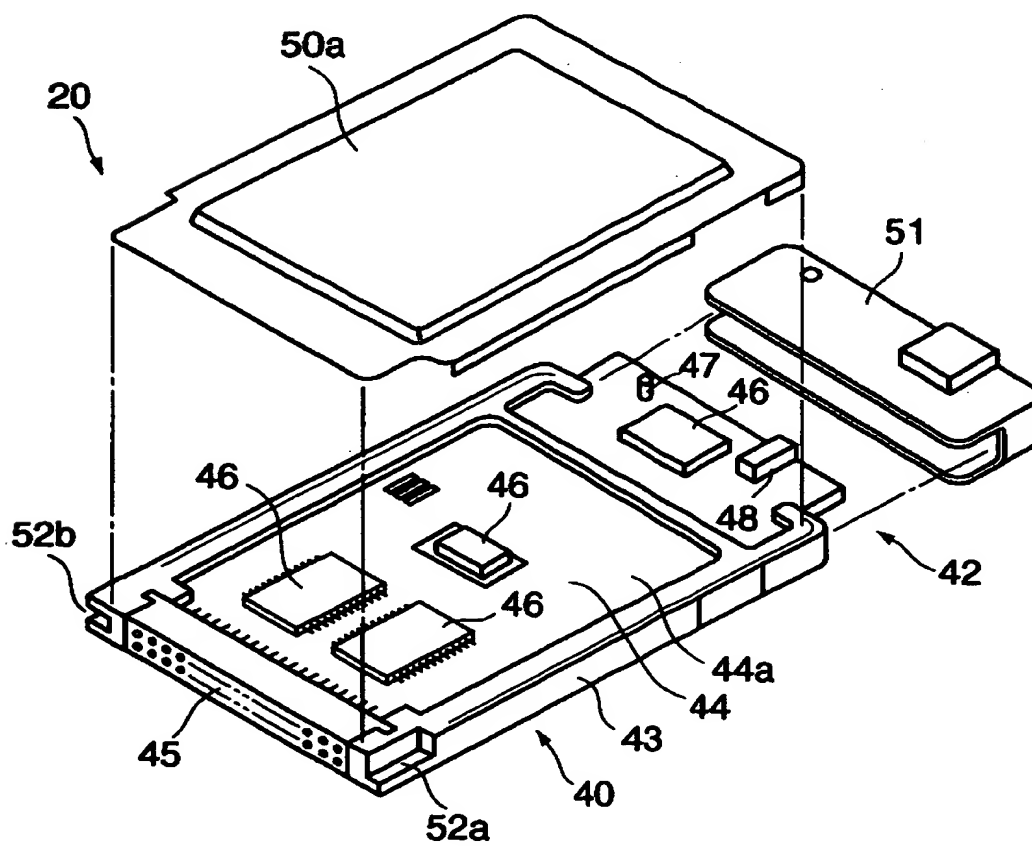
【図 6】



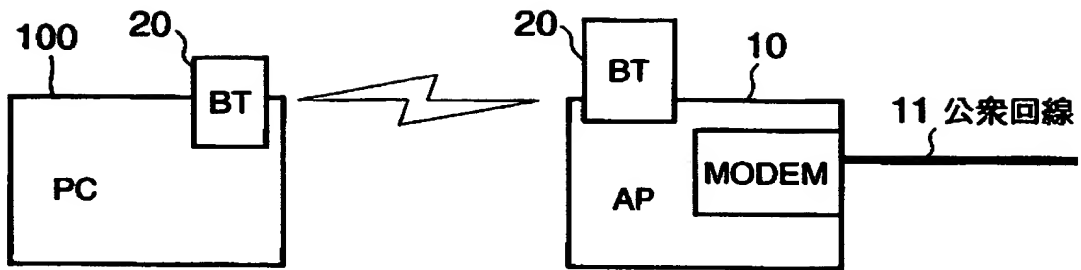
【図 7】



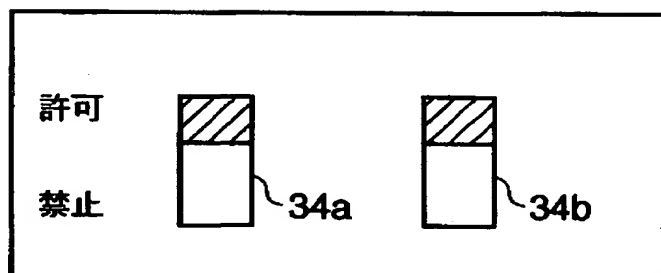
【図 8】



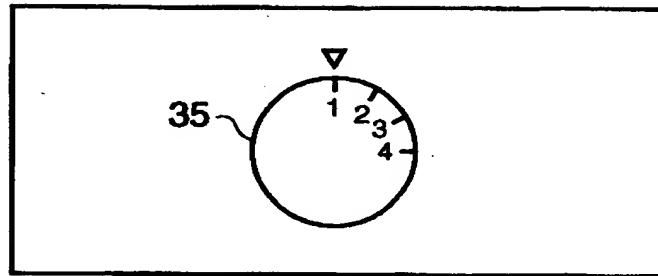
【図 9】



【図 1 0】



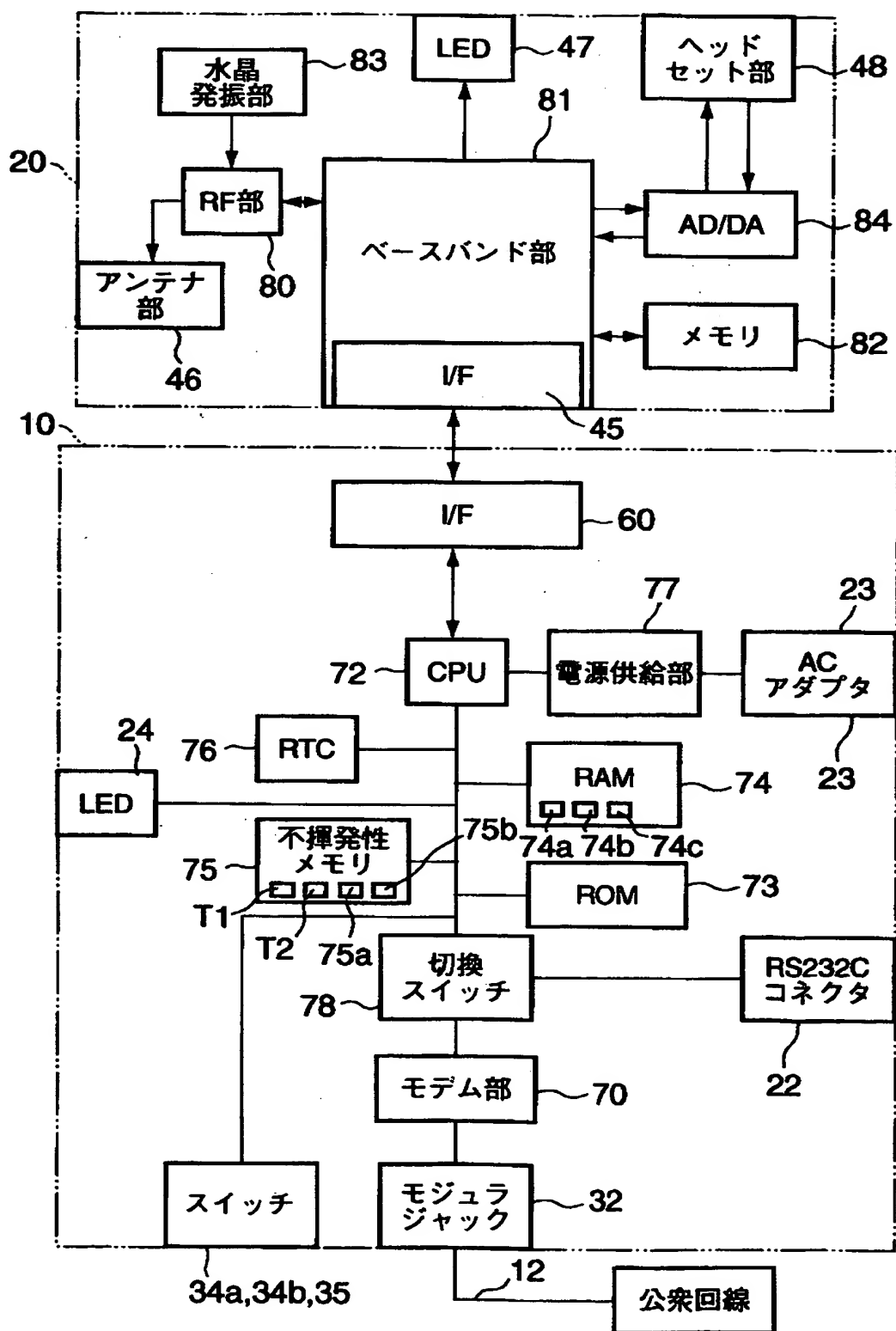
【図 1 1】



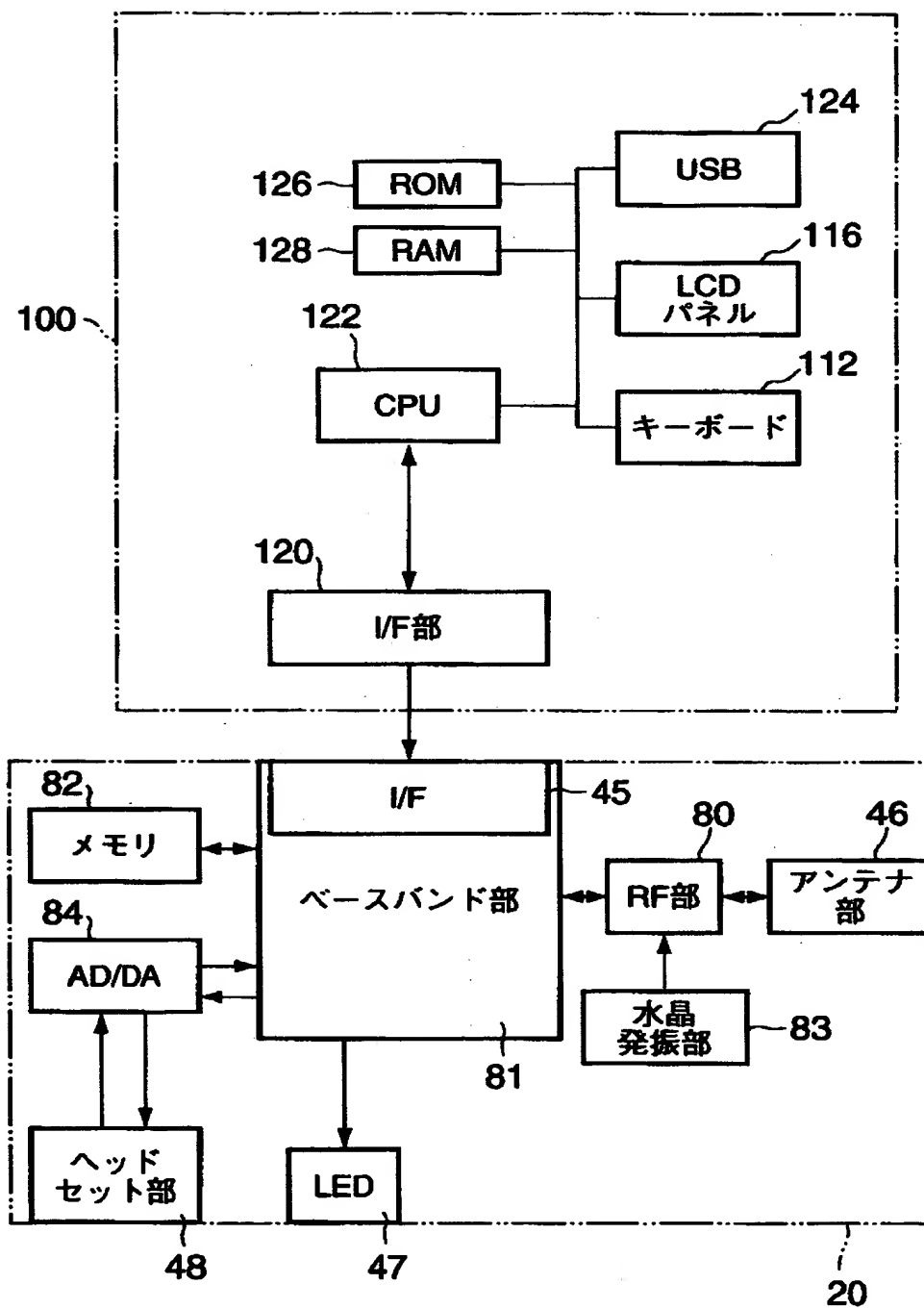
【図 1 2】

SW1	SW2	ロータリスイッチ
OFF	OFF	1
ON	OFF	2
OFF	ON	3
ON	ON	4

【図 13】



【図14】



【図 1 5】

T1 リンクテーブル

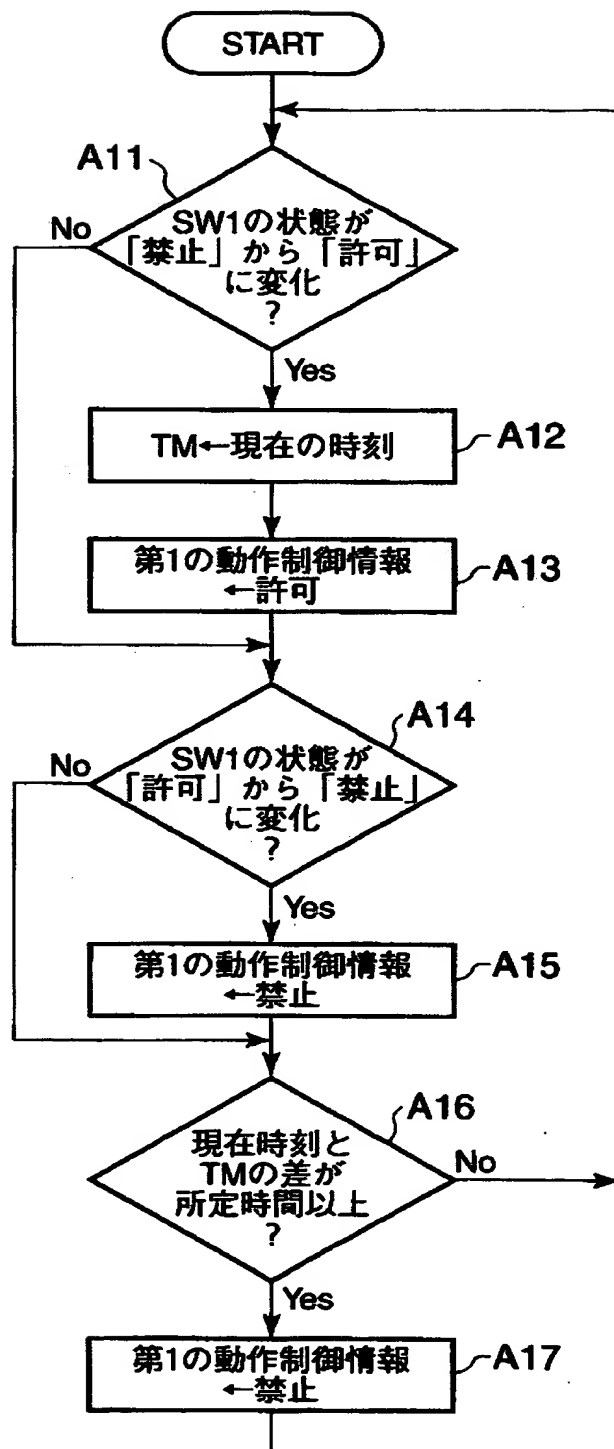
番号	ID (Hex)	リンクキー	最終接続時刻	データ有無 有/無
1	A36B35	XXXXXX	2000/07/20/12:00:10	有
2	4B3346	xxxxxx	2000/05/20/11:00:07	有
N-1	87647A	oooooo	2000/08/12/16:30:37	有
N	—	—		無

【図 1 6】

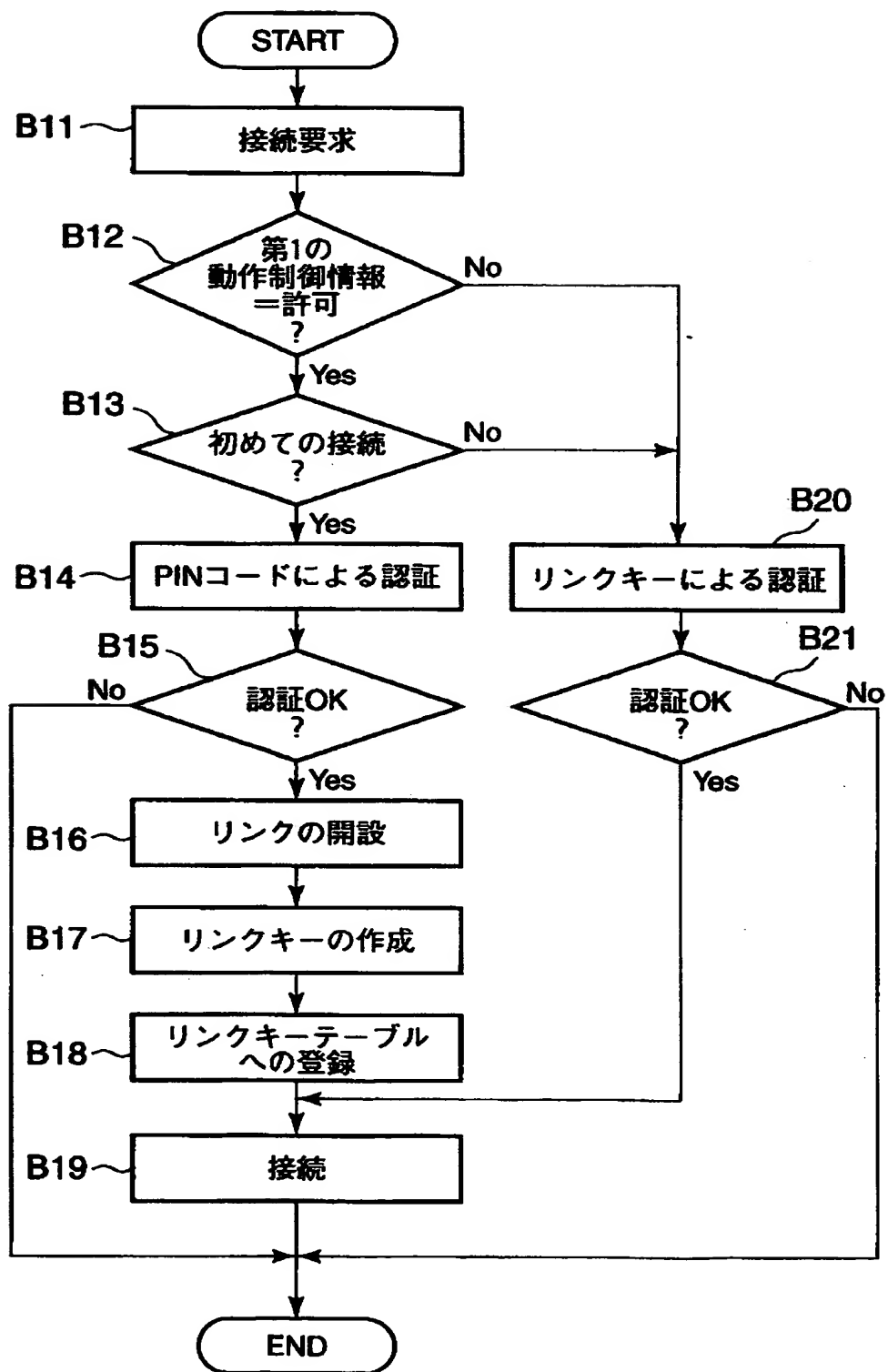
T2 認証エラーテーブル

番号	ID (Hex)	認証エラー回数	最終接続時刻	データ有無 有/無
1	A36B35	2	2000/07/20/12:00:10	有
2	4B3346	5	2000/05/20/11:00:07	有
M-1	87647A	1	2000/08/12/16:30:37	有
M	—	—		無

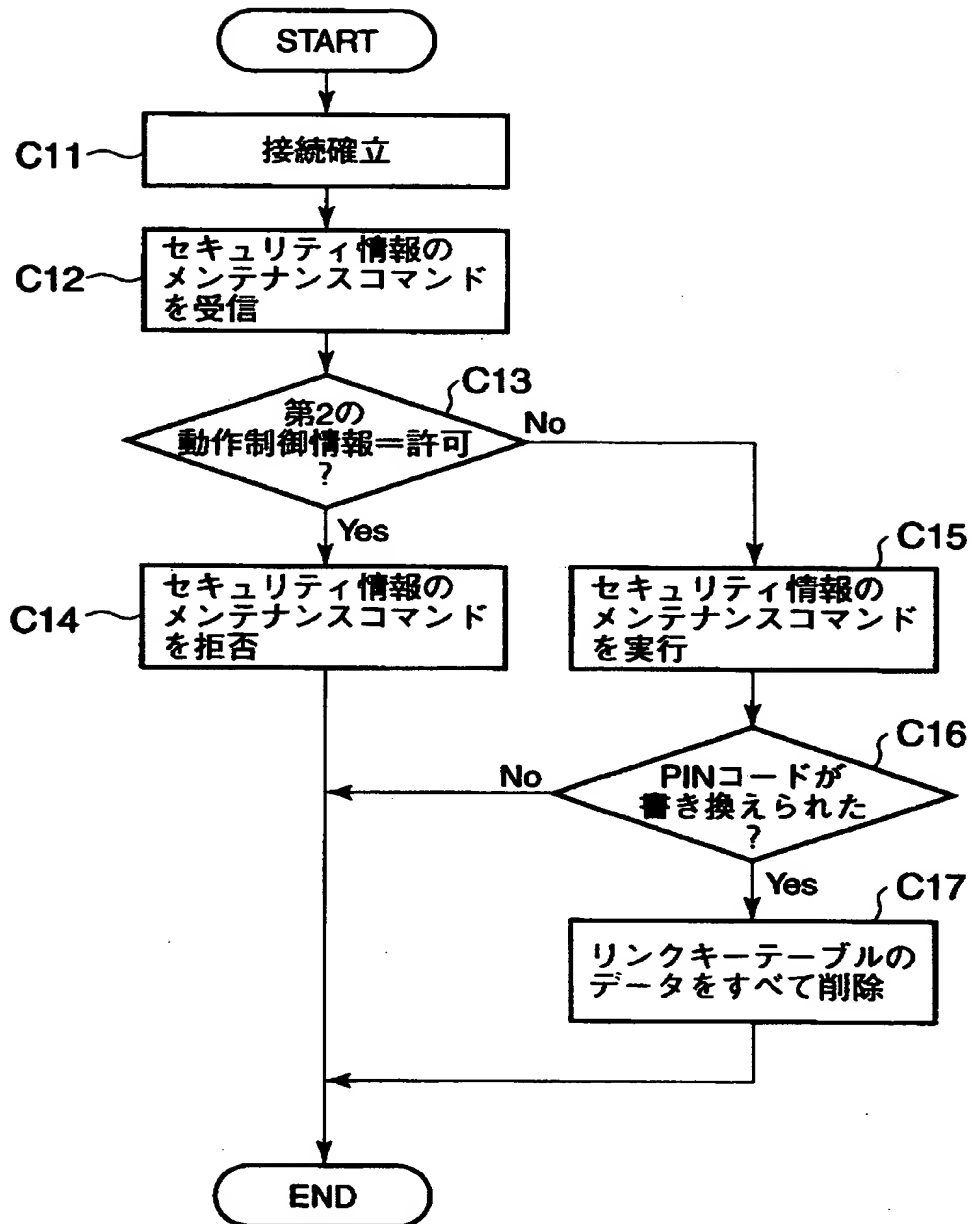
【図17】



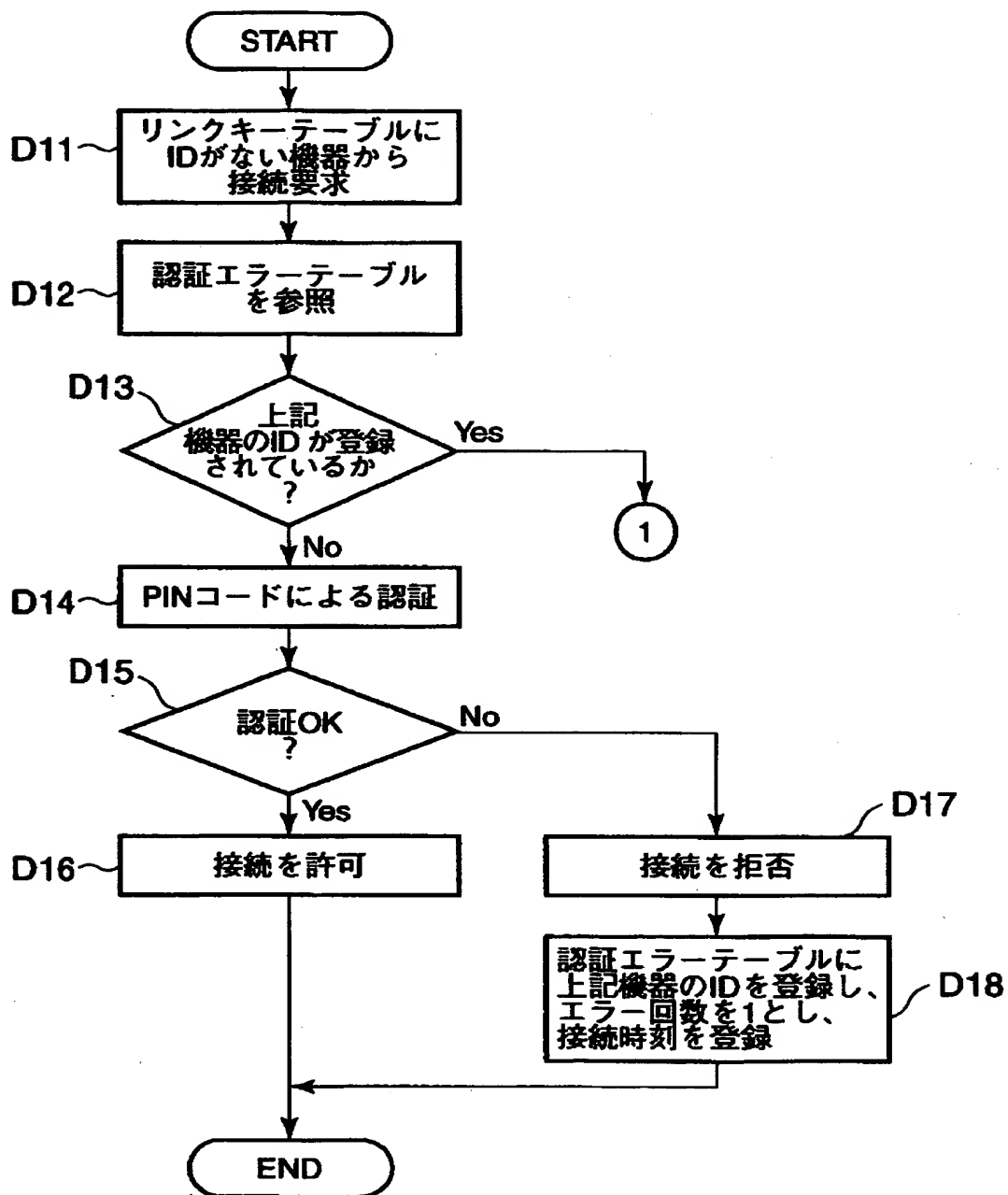
【図18】



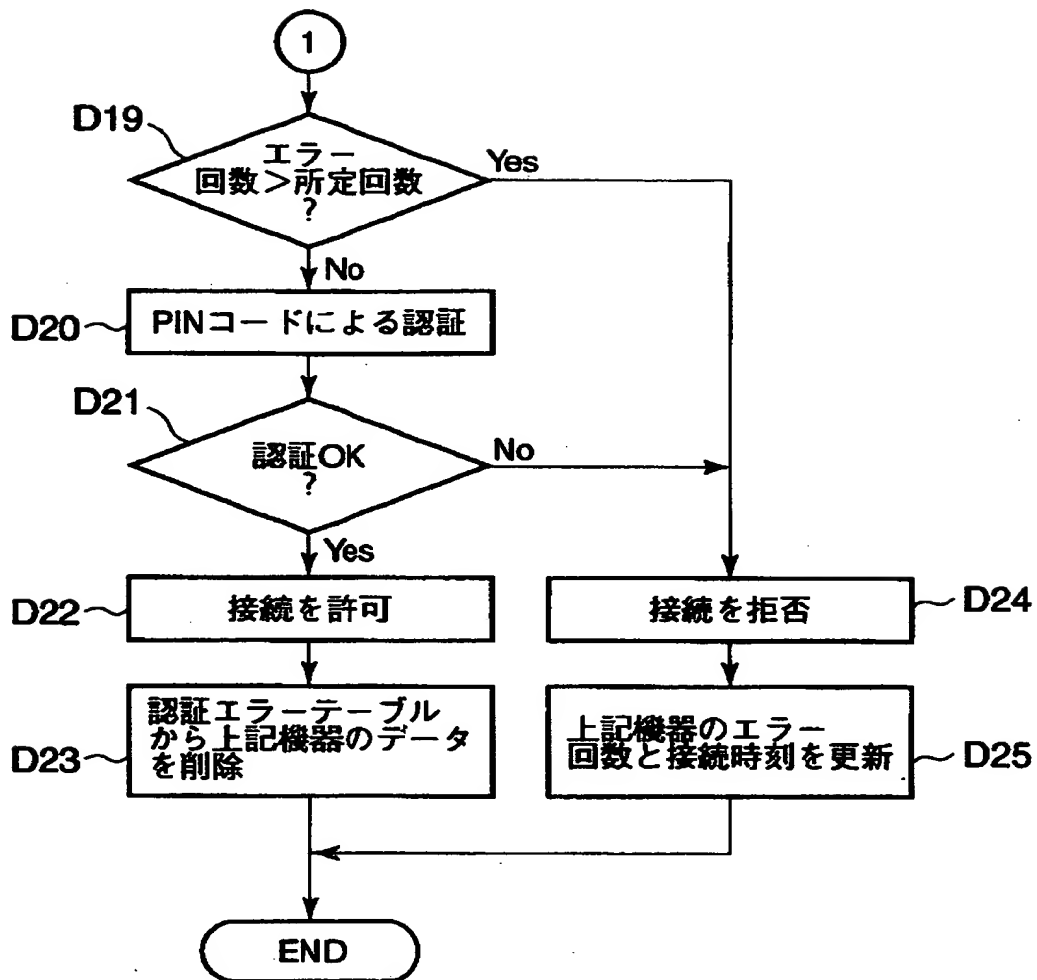
【図19】



【図20】

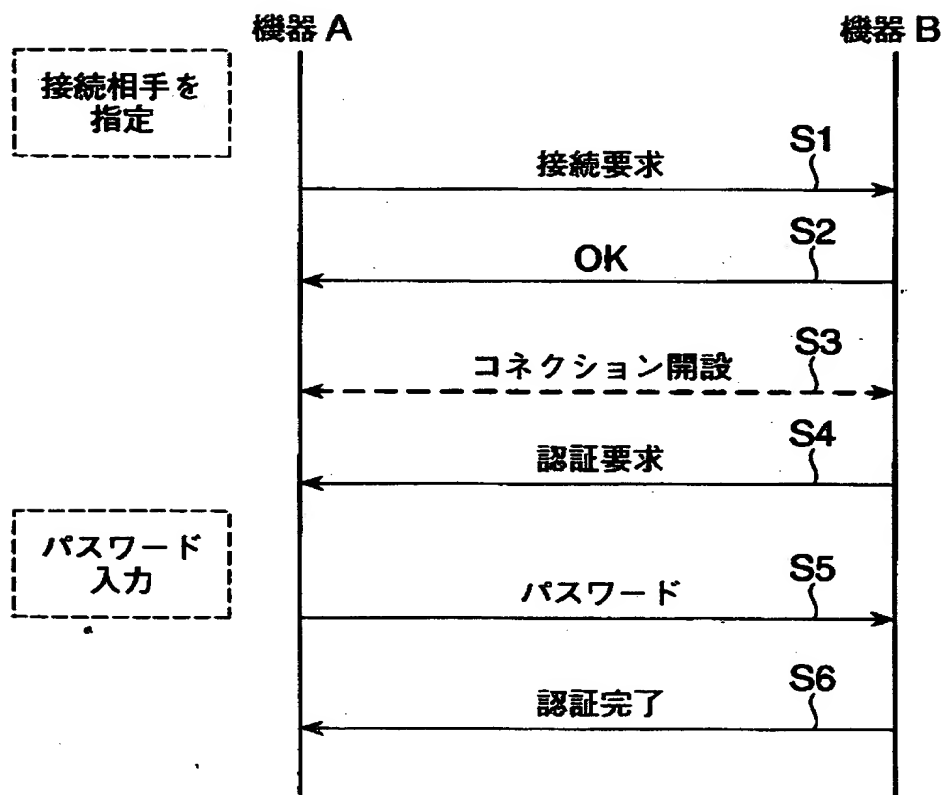


【図 21】



【図 22】

〔接続要求から認証完了までの流れ〕



【書類名】 要約書

【要約】

【課題】他の機器からの不正アクセスを防止してセキュリティを確保する。

【解決手段】機器本体にスイッチを設け、このスイッチが許可状態に切り換えられた場合には、特定の識別コード（PINコード）による認証を許可し（ステップA11～A13）、スイッチが禁止状態に切り換えられた場合には上記特定の識別コードによる認証を禁止する（ステップA14、A15）。これにより、普段はスイッチを禁止状態にしておくことで、不正アクセス者が特定の識別コードを用いてアクセスすることを防ぐことができる。また、スイッチが許可状態にあるときから所定時間経過した場合に、上記特定の識別コードによる認証を禁止する（ステップA16、A17）。これにより、スイッチを許可状態にした後で禁止状態に戻し忘れたとしても、不正アクセスを防いで機器のセキュリティを確保できる。

【選択図】 図17

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝